MADRAS FERTILIZERS LIMITED

(A GOVT. OF INDIA UNDERTAKING)
MANALI, CHENNAI 600 068
E Mail epromfl@gmail.com,epro@madrasfert.co.in
TELEPHONE: 044 25945 318, 25945 319

NOTICE INVITING TENDER FOR

Procurement of Desktop Computers & Related Components, with an Onsite warranty of 3 years at MFL

TENDER No. ESER/MIS/MIS-DESKTOP/ 150424/002 dated 15-03-0024

SUMMARY

Online bids are invited from reputed Service Providers **for Procurement of Desktop Computers & Related Components with an onsite warranty and support for a period of three years at MFL.** Bidders, who are interested to submit bids, may visit MFL website www.madrasfert.co.in ["Tenders"] or Central Public Procurement web http://eprocure.gov.in/eprocure/app **Instructions for applying e-Tendering are given in Annexure-1.**
For any clarification, please communicate to the following:

Eprocurement cell	**epro@madrasfert.co.in/epro1@madrasfert.co.in**	
Phone	**044 25945318/25945319** **Mr K Mohamed Easak**	
User contact details	venki@madrasfert.co.in	044-25945280
	ssmp@madrasfert.co.in	044-25945282

Tender No. & Date and Description	
ESER/MIS/MIS-DESKTOP/150424/002 dated 15-03-0024 for Procurement of Desktop Computers & Related Components with an onsite warranty and support for a period of three years at MFL.	
Estimated Contract Value	49 lac(including tax)
Nature of Bidding	Two Part Bidding : 1st Part : EMD,Techno-Commercial Bid 2nd Part: Price Bid
Commencement of viewing and downloading tender document from e-Tender Website	15/03/2024
Due date & Time of submission (Electronic bid to be submitted in e-Tender website)	15/04 /2024 on or before 16:00 Hours
Technical Bid Opening Date & Time	16/ 04 /2024 @ 14:00 Hours
Bid Submission	Three Separate on-line bids

(To be uploaded on or before the due date and time meant for uploading of bids)	1. EMD 2. Techno-Commercial bid 3. Price Bid To be submitted with price break up details per Price Bid Format (Annexure-5) on or before the date & time meant for submission of bids
Procedure for Decryption of Online Bid	Bids will be opened in seriatim viz., EMD, Techno-Commercial Bid and Price Bid. Online bids without scanned copy of the NSIC/MSEs Certificate, Insurance Surety Bond /BG/e-BG/RTGS will be rejected
Bid Validity	120 days from the due date of decryption of bids.
Price Bid Opening Date	Techno-Commercially Qualified Tenderers only will be intimated
EMD	**EMD Amount** **EMD Amount**: **Rs.1,00,000/-**(EMD payment can be made in the form of DD/BG/e-BG/RTGS/ Insurance Surety Bond. (Ref.Annexure-14 - EMD terms & conditions and Anexure-15 - EMD BG Format). Scanned copy of the EMD DD/BG/e-BG//RTGS/ Insurance Surety Bond. remittance details should be uploaded as part of the offer along with Techno-Commercial bid. Original EMD by way of DD/BG or proof for submission thru RTGS (UTR number) should be furnished in a separate sealed cover super scribed as EMD for TENDERNo. ESER/MIS/MIS-DESKTOP 150424/002 dated 15/03/2024 and the same should be addressed to the DGM-MIS and should reach MFL within three working days from the due date of opening the tender. **Bidders with Start-up/NSIC/MSE's with certificates seeking exemption (only for EMD)** from payment of EMD should upload such valid certificate along with their bid before the closing date and time of tender. If such valid certificates are not uploaded along with their bid before the closing date and time of tender, their bids will not be considered. Any other guideline as issued by GOI from time to time is applicable
Security Deposit (SD)	5% of the Contract Value in the event of Award of Contract
Mode of Payment for SD	By Demand Draft in favour of Madras Fertilizers Ltd., payable at Chennai or thru

	RTGS as per (Annexure – 11) or by Bank Guarantee (Annexure – 10 for SD) or Insurance Surety Bond
BG Validity	For SD 90 days after the date of completion of contract.
Payment Term	**60 days (for MSE 45 says) Credit Payment only** through RTGS on receipt of the bill free from the defect, subject to our acceptance, if any
Period of Warranty / Support	The onsite warranty and support is valid for a period of **three years** from the date of completion of work in all aspects.
Time schedule	The work has to be completed in all respects within 6 weeks from the date of placing a final confirmed Purchase/Work Order.
Bid Evaluation Basis	Techno-Commercially qualified **overall L1** basis on normal circumstances
Negotiation / Reverse Auction	Will be conducted, If required

DEPUTY GENERAL MANAGER– MIS
MADRAS FERTILIZERS LTD
MANALI
CHENNAI 600 068

List of Annexures

ANNEXURE - 1

INSTRUCTIONS TO TENDERERS FOR APPLYING E-TENDER

1.1 **Instructions to the Tenderers / Bidders for the e-submission of the bids online through the e-tender site of M/s National Informatics Centre (NIC)**

1.1.1 Bidders should do the registration in the tender site http://eprocure.gov.in/eprocure/app using the option available (online bidder enrolment). Then the Digital Signature registration has to be done with the e-token, after logging into the site. The e-token may be obtained from one of the authorised Certifying Authorities such as n-Code / e-Mudhra /safe script.

1.1.2 Bidder then need to login to the site through their user ID / password chosen during registration.

1.1.3 The e-token that is registered should be used by the bidder only and should ensure safety of the same.

1.1.4 The Bidders can update well in advance, the documents such as certificates, purchase order details etc., and these can be selected as per tender requirements and then send along with bid documents during bid submission.

1.1.5 After downloading / getting the tender schedules, the Bidder should go through them carefully and then submit the documents as asked, otherwise, the bid will be rejected.

1.1.6 If there are any clarifications, this may be obtained online through the tender site, or through the contact details. Bidders should take into account the Corrigendum published before submitting the bids online.

1.1.7 Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender schedule and they should be in .pdf / .xls /.jpeg/.rar formats only.

1.1.8 Vendors of NSIC / MSEs can claim exemption from EMD on submission of valid proof of documents obtained from NSIC/MSEs.

1.1.9 Offers without valid NSIC / MSEs Certificate, will be rejected.

1.1.10 It is construed that the bidder has read all the terms and conditions before submitting their offer including General Terms & Conditions (GTC) and Special Terms & Conditions (STC).

1.1.11 The bidder has to submit the tender document online well in advance before the prescribed time to avoid any delay or problem during the submission process.

1.1.12 After the bid submission, (the bid token number) given by the e-tendering system should be printed by the bidder and kept as a record of evidence for online submission of bid for the particular tender.

1.1.13 The Tender Inviting Authority (TIA) will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders.

1.1.14 The tendering system will give a successful bid updation message after uploading all the bid documents submitted and then a bid summary will be shown with the bid number, date and time of submission of the bid with all other relevant details. The documents submitted by the bidders will be digitally signed using the e-token of the bidder and then submitted.

1.1.15 The bid summary has to be printed and kept as an acknowledgement as a token of the submission of the bid. The bid summary will act as a proof of bid submission for a tender floated and will also act as an entry point to participate in the bid Decryption date.

1.1.16 Bidder should log into the site well in advance for bid submission so that he submits the bid in time, i.e., on or before the bid submission end time. If there is any delay, due to other issues, bidder only is responsible.

1.1.17 Each document to be uploaded through online for the tenders should be less than 8 MB. However, if the file size is less than 8 MB, the transaction uploading time will be very fast. The total size of the documents in all the covers put together, should be less than or equal to 8 MB.

1.1.18 The bidder should see that the bid documents submitted should be free from virus and if the documents could not be opened, due to virus, during tender Decryption, the bid is liable to be rejected.

1.1.19 The time settings fixed in the server side and displayed at the top of the tender site, will be valid for all actions of requesting, bid submission, bid Decryption etc., in the e-tender system. The bidders should follow this time during bid submission.

1.1.20 All the data being entered by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered will not viewable by unauthorized persons during bid submission and not be viewable by any one until the time of bid Decryption. Overall, the submitted tender documents become readable only after the tender Decryption by the authorized individual.

1.1.21 The confidentiality of the bids is maintained since the secured Socket Layer 128 bit encryption technology is used. Data storage encryption of sensitive fields is done.

1.1.22 The bidders are requested to submit the bids through online e-tendering system to the TIA well before the bid submission end date & time (as per Server system clock).

1.1.23 The bidder should log out of the tendering system using the normal log out option available at the top right hand corner and not by selecting (X) exit option in the browser.

1.1.24 Bidders should ensure that prices should not be indicated anywhere in the un-priced part. The prices should be indicated only in the price bid and nowhere else.

1.1.25 Bidders to note that if prices are indicated in their un-priced Techno-Commercial part their offer will be rejected and NO further evaluation or communication will be entertained in this regard.

1.1.26 Bidders to note that the very act of using DSC for downloading the bids and uploading their offers shall be deemed to be a confirmation that they have read all sections of the pages of the bid document including General Conditions of Contract without any exception and have understood the entire document and are clear about the requirements of the tender requirements.

ANNEXURE -2

1. Pre-Qualification Criteria

- The Tenderer should be a company /firm registered in India

- Tenderer shall have a fully functional office at Chennai with more than 10 years of operation for smooth coordination and support **(Proof to be produced)**

- The Tenderer to be valid ISO 9001-2015 certified company

- The Tenderer shall be an authorized platinum partner (Solution Provider) of DELL / Lenovo / HP and to be a platinum partner for last three consecutive years **(Proof to be produced)**

- The OEM partner should have a manufacturing facility in India (proof to be submitted)

- The Tenderer must have a business turnover of minimum of 10 Cr. Per annum. (Proof to be attached for the last 3 years **(Audited Results for financial years 2020-21,2021-22,2022-23)**

- Must have minimum of 5 years of experience in the relevant field in supply and installation of Desktop Computers (Submit one Desktop PO and One Central Endpoint Advanced (SOPHOS AV) PO **on or before March 2018 (Proof to be produced)**

- The vendor should have an experience in installation and maintenance of desktop computers/ Anti-Virus in a Large GOVT Organizations like **STATE/CENTRAL/PSU's** (Submit one Desktop and SOPHOS AV related Purchase Order within last 3 years. PO date should be on or after January-2020) **(Proof to be produced)**

- The tenderer should have at least one certified engineer who has experience in" Sophos central endpoint and server**" (Proof of certificate with employee name & ID Card to be submitted)**

- Tenderer to be a partner of SOPHOS products **(Proof to be produced)**

- If the Tenderer is under Holiday List / De-list or having any litigation with MFL, they need not apply. Tenderer shall submit Self-declaration as given in **Annexure -6** of NIT

- Also, if the Tenderer is under Black List in any State / Central Government or other PSUs, then they need not apply. Tenderer shall submit Self-declaration as given in **Annexure -6** of NIT

  If any of the above documents is not available, MFL may reject the tender and will not be considered for further processing

ANNEXURE-3

Technical information

1. Objective

- Supply & Installation of Desktop Computers in MFL Head office and Regional offices with an onsite warranty and support for a period of three years

2. Place of Work

- Head Office, Manali, Chennai-68 and Regional offices as per Annexure 12

3. Scope of Work

- Installation of Desktop in MFL & Regional Office, City office and Delhi office as per MFL requirements
- Installation of Sophos Central Anti-virus in All desktop as per MFL requirements
- Installation of other software (office/Acrobat/etc..) in a selected Desktops as per MFL requirements
- Training & Documentation will be provided to MFL employees related to the above Products
- All Installation to be done by OEM or OEM's Authorized Partner only

4. Detailed Description of Work

- Install Windows 11 Professional Operating systems in all Desktops and configure existing browser based MFL ERP(OLIS) as well as Future ERP SAP HANA
- After installation of Windows-OS in Desktop copy all existing important files from old computers to new PC as per MFL requirements.
- Install free Mail client software and connect to MFL Zimbra mail server (Windows Live mail / General mail client) in All desktop with copy of old address book, mails etc. as per MFL Requirements
- Installation of Sophos Antivirus in all desktop as per MFL requirement and connect to existing SOPHOS XGS-2100 Firewall for more protection like RANDSOMWARE / END Point security / Auto update without ADS / DLP /Web Advisor/USB Blocking etc.
- All desktop are connected to workgroup with different IP address and should support MFL File servers (Windows 2019/windows 2003) for network sharing
- Some Desktop will be delivered to MFL Regional offices as per annexure-12, at Vendor scope & responsibility after installation of Software etc.

4.1 Other Terms and Conditions

Response time should be immediate in case of problem

In case of emergency, the vendor will support 8X5 either thru remote or onsite

Acceptance for upgrades / patches / patch sets needs to be sourced, delivered & installed by the vendor in time and clear logs caches etc.,

The vendor should complete the project as per MFL requirement without any argument

5 Product Specifications

5.1 Desktop Computers – 100 NOS

Sno	Component	Description	Complied (Yes/No)
1	**Make & Model**	**DELL /HP/LENOVO**	
2	Chipset	Intel B660 or higher	
3	Form Factor	Mini Tower / Tower model /SFF	
4	Configured CPU	Intel Core i3-12100,3.30 to 4.30 GHZ, 12MB Cache, 4 Cores or higher	
5	Memory slots	Two DDR4 DIMM slots, speeds 3200 MHZ or higher	
6	Memory Size	16 GB 8+8 or higher (should scale up to 64 GB)	
7	Audio Port	One universal audio jack	
8	Storage	256-GB or higher in size (PCIe® NVMe™ M.2 SSD)	
9	Key board	104 keys with Rupee font OEM make	
10	I/O slots	Front Side - Two USB 2.0, Two USB 3.2 Gen 1 port Rear Side – Two USB 2.0 with smart power on, Two USB 3.2 Gen 1 port or more	
11	Ethernet ports	10/100/1000 Mbps LAN or higher speed with on board	
12	Power Supply	Minimum 180 watts Power Supply or higher	
13	PCI SLOTS	At least Two PCI slots and One PC Express Slots or more	
14	MONITOR	20 inch LED Full HD or higher in size, one HDMI , one VGA port with necessary cable etc. with OEM make	
15	Video Port on CPU	One Display port 1.4a(HBR2) and HDMI1.4b & 1 VGA or more	
16	Power cord	Indian 3 pin power cable	
17	Mouse	OEM Wired Optical Mouse	
18	Colour specification	All CPU, Monitor, Keyboard, Mouse & cables in Black color only	
19	Operating system	OEM Operating System with latest service pack (Microsoft Windows 11 Professional 64 bit) upgrade to windows 12 with one media	
20	Warranty	3 years On-site Comprehensive hardware support	

5.2 Sophos Antivirus client Specification – 100 NO

Sl.no	Component	Description	Complied (Yes/No)
1	**Make & Model**	**INTERCEPT X – Advanced (Managed by SOPHOS Central)**	
2	Evaluation	**MITRE Attack Evaluation**	
3	**AV Features**	**AV-Test Certification**	
4		**Integrated Management**	
		Must have a unified console for managing multiple products such as Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control etc.	
		All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles.	
5		**Multi-Platform Management**	
		Windows, Mac, and Linux machines must be managed from one management console.	
6		**Updating Bandwidth Consumption**	
		Updating of endpoints should have the ability to set pre-configured available bandwidth used for both software updating and threat definition updates(e.g., 64, 128, 256Kbps, etc.)	
		Must have the option to set up a local cache updating server within the on-premise network environment to minimize large software engine update.	
		Must have an Update Management Policy that contains the configuration of update schedules on managed endpoints.	
7		**Deployment Options**	
		Deploying the endpoint agent must support the following methodology:	
		1) Email setup link	
		2) via AD Startup/Shutdown script	
		3) AD Login script	
		4) SCCM	
		5) Include the endpoint agent installation to a gold image	

8		**SIEM Integration**	
		Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM.	
9		**API for Endpoint Management**	
		Must have APIs offered as RESTful HTTP endpoints over the public internet.	
		APIs must have the capability to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically.	
		Must have an API that can run osquery against endpoints connected to the admin console.	
		Must have an API that can run XDR queries against the Data Lake.	
10		**Role Management**	
		Must have the capability to allow the separation of estate management to different administrator login.	
		Must provide admins the capability to assign predefined administrative roles to users who need access to the Admin Console.	
		Must be able to create custom roles and assign the products and access needed.	
11		**Microsoft AD Synchronization**	
		Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers to the Cloud Dashboard for policy management.	
12		**Federated Sign-In**	
		Must support the following Identity Providers (IDP):	
		Azure AD	
		Open ID (Okta)	
		Microsoft AD FS	
13		**Device Group Discovery**	
		Must be able to compare devices that have the vendor endpoint protection agents installed with devices synchronized from Active Directory and list the unmanaged devices so that you can install protection on them.	
14		**Account Health Check**	

		The admin console must have an Account Health Check section where you can see whether you're using all the protection features included in your license.	
15		**Policies**	
		Selected policies should be able to be applied to either users or devices.	
		Policies must have the capability to be disabled automatically based on a scheduled time and date.	
16		**Enhanced Tamper Protection**	
		Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection.	
		Must have the capability to prevent the following actions on the endpoint protection solution:	
		1) Stopping services from the Services UI	
		2) Kill services from the Task Manager UI	
		3) Change Service Configuration from the Services UI	
		4) Stop Services/edit service configuration from the command line	
		5) Uninstall	
		6) Reinstall	
		7) Kill processes from the Task Manager UI (desired)	
		8) Delete or modify protected files or folders	
		9) Delete or modify protected registry keys	
		Must be able to export Tamper Protection passwords in CSV or PDF formats.	
17		**Threat Protection**	
		Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint.	
		Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops regardless of their nature or the concealment mechanisms used.	
		Must protect against threats related to executable files, as well as document files containing active elements such as macros or scripts. It must protect against exploits resulting from discovery (whether published or not) of security flaws in systems or	

		software.	
		Must have the capability to 'lookup' files in real-time to verify if they are malicious. This feature checks suspicious files against the latest malware in the vendor's Threat Intelligence database in the cloud.	
		Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. Access must be denied unless the file is healthy.	
		Must have the capability to do real-time scanning of end-users Internet Access. It must monitor and classify the Internet websites according to their level of risk, and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must be proactively blocked by the solution to prevent any risk of infection or attack against a flaw of the browser used. The solution must carry out checks against a database of compromised websites that are constantly being updated with new sites identified per day.	
		Must protect managed systems from malicious websites in real-time, whether end-users work within the company or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.)	
18		**Anti-rootkit Detection**	
		Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.	
19		**Suspicious Behavior Detection**	
		Must be able to protect against unidentified viruses and suspicious behavior.	
		Must have both pre-execution behavior analysis and runtime behavior analysis.	
		Must be able to identify and block malicious programs before execution.	
		Must be able to dynamically analyze the behavior of programs running on the system and detect then block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted.	
		Must provide protection against buffer overflow attacks	

20		**Scanning**	
		Must provide a scheduled scanner to run depending on the selected frequency or by manually triggering through Windows Explorer to scan the specified directories (local, remote or removable), with analysis parameters used, which may be different from the ones selected for real-time protection.	
		Must have the capability to scan archives such as zip, cab, etc. which can be enabled via policy settings.	
21		**Advanced Deep Learning Mechanism**	
		The system must have light speed scanning; within 20 milliseconds, the model shall able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.	
		Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.	
		Must protect the system even when offline and will not rely on signatures.	
		Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables.	
		Able to perform new Zero days threat scanning offline (without internet).	
		Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.	
		Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up-to-date.	
		Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance.	
		The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn.	
22		**Exploit Prevention/Mitigation must detect and stop the following known exploits:**	
		1) Enforcement of Data Execution Protection (DEP) Prevents abuse of buffer overflows	
		2) Mandatory Address Space Layout Randomization (ASLR)	

		Prevents predictable code locations	
		3) Bottom-up ASLR *Improved code location randomization*	
		4) Null Page (Null Dereference Protection) *Stops exploits that jump via page 0*	
		5) Heap Spray Allocation *Reserving or pre-allocating commonly used memory addresses, so they cannot be used to house payloads.*	
		6) Dynamic Heap Spray *Stops attacks that spray suspicious sequences on the heap*	
		7) Stack Pivot *Stops abuse of the stack pointer*	
		8) Stack Exec (MemProt) *Stops attacker's code on the stack*	
		9) Stack-based ROP Mitigations (Caller) *Stops standard Return-Oriented Programming attacks*	
		10) Branch-based ROP Mitigations (Hardware Augmented) *Stops advanced Return-Oriented Programming attacks*	
		11) Structured Exception Handler Overwrite Protection (SEHOP) *Stops abuse of the exception handler*	
		12) Import Address Table Access Filtering (IAF) (Hardware Augmented) *Stops attackers that lookup API addresses in the IAT*	
		13) LoadLibrary API calls *Prevents loading of libraries from UNC paths*	
		14) Reflective DLL Injection *Prevents loading of a library from memory into a host process*	
		15) Shellcode monitoring *Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null free encoding*	
		16) VBScript God Mode *Have the ability to detect the manipulating of the safe mode flag on VBScript in the web browser*	
		17) WoW64 *Must have the ability to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while still enabling the WoW64 layer to perform this transition.*	
		18) Syscall *Stops attackers that attempt to bypass security hooks*	

		19) Hollow Process Protection *Stops attacks that use legitimate processes to hide hostile code*	
		20) DLL Hijacking *Gives priority to system libraries for downloaded applications*	
		21) Application Lockdown *Will automatically terminate a protected application based on its behavior; for example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas; the solution must block the malicious action – even when the attack doesn't spawn a child process.*	
		22) Java Lockdown *Prevents attacks that abuse Java to launch Windows executables*	
		23) Squiblydoo AppLocker Bypass *Prevents regsvr32 from running remote scripts and code*	
		24) CVE-2013-5331 & CVE-2014-4113 via Metasploit *In-memory payloads: Meterpreter & Mimikatz*	
		25) EFS Guard *Can protect files that are encrypted with EFS from Encrypting File System attacks*	
		26) CTF Guard *Prevents abuse of the CTF subsystem*	
		27) ApiSetGuard *Helps prevent an application from side-loading a malicious DLL that poses as an ApiSet Stub DLL*	
23		**Advanced Exploit Mitigation**	
		Must be able to prevent the hijacking of legitimate applications by malware such as the following:	
		Process hollowing attacks	
		DLLs loading from untrusted folders	
		Credential theft	
		Code cave utilization	
		APC violation	
		Privilege escalation	

24		**Malicious Traffic Detection (MTD)**	
		Must be able to detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.	
25		**Intrusion Prevention System (IPS)**	
		Must be able to prevent malicious network traffic with packet inspection (IPS).	
		Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.	
26		**Anti-Ransomware Protection**	
		Must have the ability for the encrypted files to be rolled back to a pre-encrypted state.	
		Both Anti-Exploit and Ransomware protection does not need to have a Cloud Lookup to perform the detection.	
		When the Anti-crypto function suspects that certain behavior is not in keeping with its intended process, the Data Recorder starts caching data while the said behavior is closely reviewed to identify if the application is legitimate or if the activity is warranted.	
		The anti-crypto function shall look back at all the malicious file modifications made by that process and restores them to their original location.	
		Should a ransomware infection managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported (RCA).	
		Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk.	
27		**AMSI Protection**	
		Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI).	
		Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged.	
28		**Data Loss Prevention (DLP)**	
		Must be able to monitor and restrict the transfer of	

		files containing sensitive data.	
		Must have the capability to create custom DLP policies or policies from templates.	
		Must have DLP policy templates that cover standard data protection for different regions.	
29		**Peripheral Control**	
		Must have the capability to control and restrict removable mass storage devices (USB sticks, CD Rom, USB external hard drives, iPods, MP3 players, etc.), as well as connection devices (Wi-Fi, Bluetooth, Infrared, Modems, etc.).	
		Must have the capability to add device exemptions either by Model ID or Instance ID.	
30		**Application Control**	
		Must have the capability to limit the applications needed for specific user groups.	
		Must be able to detect and block application categories that may not be suitable for use in an enterprise environment.	
		Must have application categories for commonly used applications.	
31		**Web Control**	
		Must be able to block risky downloads, protect against data loss, prevent users from accessing web sites that are inappropriate for work, and generate logs of blocked visited sites.	
		Must have security options to configure access to ads, uncategorized sites, or dangerous downloads.	
		Must provide the administrator the ability to define "acceptable web usage" settings (defined by categories) in order to control the sites on which users are allowed to visit. Admin must have control access to websites that have been identified and classified in their own categories.	
		Must have a data loss protection option that allows the administrator to control access to web-based email and file downloads, with choices of blocking the data, allowing data sharing, or customizing this choice.	
32		**Windows Firewall Policy**	
		Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy.	

		Must be able to apply the Windows Firewall policy to individual devices (computers or servers) or groups of devices.	
33		**Root Cause Analysis**	
		Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization's security posture	
		Must be able to record chain of events that occurred after an infection has been detected, enabling you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection.	
		Shall provide a summary of the event: What exploit was discovered, where the beacon event occurred (an asset), when it occurred, how the infection succeeded. Eg. "Outlook.exe."	
		Shall provide recommendations to address the problem: Things to look for post-attack. Eg. Aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created as a result of the infections.	
		Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column.	
		There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High).	
		Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, start/stop timestamp of the event.	
		Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc. involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.	
34		**Advanced System Clean**	
		Must have the capability to trigger a deep clean upon	

		any active detection from exploit or ransomware detection.	
		The next-gen endpoint shall provide advanced Clean detection of malware by looking for the following:	
		A. Files	
		flagged as bad	
		File has been downloaded from the internet	
		Author's name/version information is missing from file properties, i.e., Impersonating a common windows system file. Reboot survivability is vigorously protected.	
		Un-common file extension used.	
		Contains PE structure anomalies and suggestions of obfuscation	
		B. Processes	
		Listening for incoming connections	
		Missing source executable file	
		No UI elements	
		Address Space Layout Randomization (ASLR) has been removed from the system.	
35		**Block Applications**	
		Must have an option to immediately detect and remove potentially malicious Portable Executable (PE) files from protected computers in the environment.	
		Must have an option to block applications using their SHA-256 hash.	
36		**On-demand Threat Intelligence**	
		Must have an option to 'request intelligence' on suspicious files, which will upload the file to our malware research team for further analysis.	
		Must be able to provide a report summary of the machine learning analysis of a suspicious file.	
		Must be able to provide a summary report with a more in-depth analysis of a suspicious file to help you decide if it's malicious or clean.	
37		**Endpoint Isolation**	
		Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case.	

		Must have an option to 'automatically isolate' compromised endpoints from the network. (not available on servers)	
38		**Forensic Data Export**	
		Must have an option to generate a Forensic Snapshot of a malicious activity that occurred on a protected endpoint.	
		Must be able to convert the generated Forensic Snapshot into a format where advanced queries can be run, such as SQLite or JSON file format.	
		Must have an option to enable audit of Windows Authentication events, which allows Forensic Snapshots to contain more information on logon events.	
		Must have the capability to upload the forensic snapshot to an AWS S3 bucket.	
39		**Live Query**	
		Must provide security analysts, and IT admins the ability to run SQL queries to answer almost any question they can think of across their endpoints and servers.	
		Must be based on Osquery that allows administrators to understand the current running state of a device.	
		Must be able to quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity via SQL queries.	
		Must let you choose which data source to use when you set up and run a query:	
		Endpoints that are currently online (90 days of data stored on the device)	
		The Data Lake in the cloud (30 days of cloud storage)	
		Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include:	
40		**IT Operations**	
		Why is a machine running slowly? Is it pending a reboot?	
		Which devices have known vulnerabilities, unknown services, or unauthorized browser extensions?	
		Are there programs running that should be removed?	
		Is remote sharing enabled? Are unencrypted SSH	

		keys on the device? Are guest accounts enabled?	
		Does the device have a copy of a particular file?	
41		**Threat Hunting**	
		What processes are trying to make a network connection on non-standard ports?	
		List detected IoCs mapped to the MITRE ATT&CK framework	
		Show processes that have recently modified files or registry keys	
		Search details about PowerShell executions	
		Identify processes disguised as services.exe	
42		**Data Lake**	
		Must be able to configure devices and supported security products to upload security data to a Data Lake and store them for 30 days so that security related information from them can be queried even if they are offline.	
		Must be able to schedule queries.	
		Data must include AWS, Azure, and GCP cloud environment API, CLI, and management console activities.	
		Must have an option to upload Android, iOS, and Chrome OS data (will require a mobile protection license from the vendor).	
43		**Microsoft 365 Integration**	
		Must be able to connect to Microsoft 365 and add its Audit log information into the Data Lake.	
44		**Remote Access**	
		Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action.	
		Must provide admins the capability to remotely connect to managed devices and get access to a command-line interface to perform actions such as:	
		Reboot a device pending updates	
		Terminate suspicious processes	
		Browse the file system	

		Edit configuration files	
		Edit configuration files	
		Must have control over which specific admin accounts have Remote Access capability.	
		Remote access sessions must be included in Audit Logs (when it started, ended or if the connection was lost)	
		Must be available on Windows, Mac, and Linux operating systems.	
45		**Suspicious Activity Prioritization**	
		Must have a detections dashboard that provides a prioritized list of suspicious activity for further investigation.	
		Suspect activities should be ranked on a 1-10 risk scale (10 being the most serious, 1 being the least), making it easy for admins to identify and focus on critical areas.	
		Each activity should include a description and provide information such as the time of the event, associated processes, executed command lines, file hashes, device, user, and much more.	
		Each activity must map to the MITRE ATT&CK framework.	
		The details of a suspicious item must be easy to take further action with a context-aware list (aka pivoting) of deeper investigation options.	
		The details of a suspicious item must be able to perform immediate actions such as running further search actions, launching a Remote Session, creating a Threat Graph, or more.	
46		***Investigations***	
		Must have an Investigations page in the admin console that groups together suspicious events reported by our Detections feature and help you do forensic work on them.	
		Must have an Investigation record that can be configured as follows:	
		Set the priority to High, Medium, or Low.	
		Change the status from Not Started to In Progress or Closed.	
		Assign an investigation to an admin account	
		Must have an Investigation Notes section where admins can add notes.	

47		**Synchronized Security**	
		Must be able to work with other security products of the vendor to share information and respond to incidents.	
48		**Endpoint + Email Gateway**	
		Must be able to automatically isolate compromised mailboxes, and clean up infected computers sending outbound spam and malware.	
49		**Endpoint + Firewall**	
		Must be able to automatically isolate infected endpoints on the public and local area networks.	
		Must be able to identify all apps on the network.	
		Must be able to link threats to individual users and computers.	
50		**Server + Firewall**	
		Must have one-touch isolation of infected servers on the public and local area networks.	
		Must be able to identify all apps on the network.	
51		**Endpoint + Wireless Access Point**	
		Must be able to restrict internet access for infected endpoints connected to Wi-Fi automatically.	
52		**Server Protection Features (will require an XDR for Servers license)**	
		includes all features above plus the following:	
53		**Automatic exclusions**	
		Must be able to automatically exclude activity by known applications (such as Microsoft Exchange and Microsoft SQL) from scanning when enabled within the policy for a server.	
54		**Application Whitelisting**	
		Must have the option to lockdown the Server and only allow approved applications to run. Controlling what can run and change an application makes it harder for attackers to hack the server.	
55		**File Integrity Monitoring**	
		Must be able to monitor system-critical files and registry keys for additional security.	
		Must have default rules that monitor changes to critical Windows system files as well as provide the	

		ability to add additional monitoring locations and exclusions via policy.	
		Must be able to monitor files, folders, registry keys, and registry values.	
56		**Cloud Security Posture Management (CSPM) Capabilities**	
		Must have CSPM capabilities that allow Admins to get details of their entire cloud infrastructure across different public cloud providers on one screen, in a single management console.	
		Must allow admins to dive directly into assets to get a more detailed asset inventory and cloud security posture.	
		Must also include the following features:	
		Cloud Asset Inventory – View a detailed inventory of your entire cloud infrastructure (e.g. IAM roles, security groups, shared storage, databases, serverless, containers and more), eliminating the need for time-consuming manual collation across AWS, Azure, and GCP.	
		Access and Traffic Anomaly Detection – Unusual login attempts, and suspicious traffic patterns are automatically detected, and teams alerted.	
		Security scans – Daily and on-demand scans monitor your cloud environment to ensure its on-going security health. Alerts are automatically prioritized by risk level, while guided response provides detailed information and instructions to resolve the issue.	
		Security Best Practice – Detect when cloud accounts and the configuration of deployed resources do not align to security best practices with Center for Internet Security (CIS) Benchmark policies, helping keep security posture at its best.	
		Alert Management Integrations – receive email notifications when manual intervention is required.	

6 Period of Contract / Warranty support

The onsite warranty and support is valid for a period of **three years (for desktops only)** from the date of completion of installation of desktops. Either party can terminate the contract by giving **one month** notice in writing. The Installation of desktops and accessories to be done within 6 weeks from the award of contract in all aspects

The contract shall be extended for a period of two more years (**SOPHOS AV Subscription alone)** with the same rate, terms and conditions with the approval of competent authority.

7 Other Terms & Conditions

- The tender dully filled in all aspects shall be signed on each page by the tenderer
- Late bid : Tenders received after due date will be rejected
- MFL reserves the right to accept or reject any or all the tenders or any part thereof without assigning any reason whatsoever
- Validity of Quote: 120 days from the date of tender opening
- MFL reserves the right to terminate the contract without notice of termination in case of any failure on the part of the contractor in discharging the services under the contract or in the event of the contractor becoming insolvent or going into liquidation. The decision of MFL in this regard shall be final and binding on the contractor and shall not be called into question
- The charges includes complete warranty of desktops and accessories
- The vendor should submit the data sheet of products as per specification (Refer point 5.1 to 5.2), if any deviation found, the tenderer will be technically dis-qualified.
- Evaluation of quotes will be on the basis of rate quoted under Annexure-5 only
- The tenderer will be selected on overall L1 basis only
- During Transit & installation period any damages of products as per vendor scope.
- Any offer received against our enquiry from sister concern, associate concern, merged company and de-merged company is summarily rejected

8. Subletting and transfer:

The Contractor shall be solely responsible for rendering any or all the services. He shall not sublet/transfer/assign the contract or any part thereof, to others. All his dealings with third parties shall be without reference, in any way to Madras Fertilizers Limited. The Contractor shall also undertake to make third parties fully aware of the position aforesaid.

The Contractor shall be responsible for all the obligations arising out of enforcement of Contract Labour (Regulation and Abolition) Act in the State. He shall also be liable to reimburse Madras Fertilizers Limited for any expenses, which the latter, as principal employer, may incur in meeting with any of the provisions of the Act.

9. Evaluation

- Evaluation of quotes will be on the basis of rate quoted under Annexure -5 only.

- The tenderer will be selected on overall L1 basis only.

STRIKE OR CESSATION OF SERVICE BY CONTRACTOR'S WORKMEN OWING TO ANY DISPUTE WITH THE CONTRACTOR PERTAINING TO WAGES OR OTHERWISE WILL NOT BE DEEMED TO BE A REASON BEYOND THE CONTRACTOR'S CONTROL AND THE CONTRACTOR SHALL PAY A PENALTY AS FIXED BY THE COMPANY FOR EACH DAY OF SERVICE STOPPAGE AND SHALL, IN ADDITION, ALSO BE RESPONSIBLE FOR ANY LOSS/DAMAGE WHICH MFL MAY SUFFER ON THIS ACCOUNT. FOR STOPPAGES OF SERVICE FOR PART OF THE DAY, PRORATA RECOVERY WILL BE MADE.

10. Negotiation / Reverse auction

Will be conducted, if required

11. SUMMARY TERMINATION

MFL reserves the right to terminate the contract due to any failure / breach of contract on the part of the contractor in discharging the service under the contract, or in the event of his becoming insolvent or going into liquidation without giving any notice. The decision of Madras Fertilizers Limited about the failure / breach of contract on the part of the contractor shall be final and binding of the contractor.

MFL also have, without prejudice to any other rights and remedies, the right in the event of the failure / breach by the contractor of any of the terms and conditions of the contract, or due to the Contractor's inability to perform as agreed for any reason whatsoever, to terminate the contract forthwith and get the work done for the unexpired period of the contract at the risk and cost of the contractor and recover the losses, damages, expenses or costs that may be suffered or incurred by MFL. The decision of Madras Fertilizers Limited about the breach/failure on the part of the contractor shall be final and binding on the contractor and shall not be called into question.
Either party can terminate the contract by giving **one month** notice in writing.

MFL reserves the right to terminate the contract without any notice in writing or without any obligation on the part of MFL in the event of MFL's decision to operate the work by a different system.

12. LAWS GOVERNING THE CONTRACT:

The contract will be governed by the Laws of India for the time being in force and as amended from time to time and the jurisdiction of the Court shall be that of the place where the Registered Office of MFL is situated.

13. ARBITRATION

Any or all disputes arising out of or in relation to this agreement shall be settled by mutual discussions and in the event of failure to do so, such dispute(s) shall be referred to the Chairman and Managing Director of MFL or any other officer nominated by him for the purpose who will be the Sole Arbitrator for settlement of such dispute(s) and whose decision shall be final and binding.

In the event of a reference made to an Arbitrator, the decision of the Arbitrator shall be final and binding on both the parties of this agreement and shall not be called into question.
Subject as aforesaid, the Arbitration & Conciliation Act 1996, shall apply to the arbitration proceedings under this Clause and such arbitration in English shall take place in the city of Chennai.

The cost in connection with arbitration shall be at the discretion of the Arbitrator who may a make suitable provision of the same in the Award.

14. LIQUIDATED DAMAGES

Since time is the essence of the order, liquidated damages @0.5% per very week of delay or part thereof subject to maximum of 5% of the contract value will be levied, if the work should not completed beyond 6 weeks.

15. DECLARATION IN HOLIDAY LIST/ BLACKLISTED / ARBITRATION PROCEEDINGS.

Where the bidder is placed in holiday list / Blacklisted by MFL or by any other Govt. PSUs, even if such bidder participated in the bidding process, their offer will not be considered for evaluation.
Where there is pending arbitration proceedings initiated by MFL against any contractor/ supplier is / are pending disposal, the offer of such contractor / supplier will not be considered for evaluation.

16. PAYMENT TERMS

Payment will be made only thru RTGS on expiry of 60 (45 for MSE) days on confirmation of successful installation of all items with all aspects (after going live) as per MFL Requirement and error free invoice subject to our acceptance.

The tenderer shall neither be entitled to claim interest for the pending bills with MFL nor the delay in payment if any, give any right to tenderer to suspend the work under the contract.

It is mandatory to upload the invoice date in GST portal by the vendor offer rising into MFL. After verifying the GST payment in GST portal, MFL will release the payments per payments terms.

17. GENERAL TERMS

The contractor shall be solely responsible for providing at his own cost, first aid, medical facilities, hospitalization, etc., in the event of any of the service personnel visiting MFL during the period of the contract sustaining any injury, meeting with accident, falling ill, or otherwise. The company is not obligated to provide any of the above facilities, if such events occur. However, upon request by the contractor the company may extend its first aid facility, or make available its ambulance for transportation to hospital or such other medical center's. The cost of such first aid, medical facility or transportation as may be determined by the company, shall be recovered from the contractor's bill

18. CARTEL FORMATION/POOL RATES

The Bidder/ Contractor/ Supplier will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to price, specifications, certifications, subsidiary contracts, submission or non-submission of bits or any other actions to restrict competitiveness or to introduce cartelization in the bidding process. Bidders found to be indulging in Cartel formation will be dis-qualified from the tender process.

ANNEXURE – 4

TECHNICAL – COMMERCIAL EVALUATION SHEET FORMAT

	Description	Yes /No
	The Tenderer should be a company /firm registered in India Tenderer shall have a fully functional office at Chennai with more than 10 years of operation for smooth coordination and support **(Proof to be produced)** The Tenderer to be valid ISO 9001-2015 certified company The Tenderer shall be a authorized platinum partner (Solution Provider) of DELL / Lenovo / HP and to be a platinum partner for last three consecutive years **(Proof to be produced)** - The Tenderer must have a business turnover of minimum of 10 Cr. per annum. (Proof to be attached for the last 3 years **(Audited Results for financial years 2020-21,2021-22,2022-23)** The vendor should have an experience in installation and maintenance of desktop computers & Anti-virus in a Large GOVT Organizations like **STATE/CENTRAL/PSU's** (Submit one Desktop and SOPHOS related Purchase Order within last 3 years. PO date should be on or after January-2020) **(Proof to be produced)** The tenderer should have at least one certified engineer who has experience in "Sophos central endpoint and server "**(Proof of certificate with employee name & ID Card to be submitted)** If the Tenderer is under Holiday List / De-list or having any litigation with MFL, they need not apply. Tenderer shall submit Self-declaration as given in **Annexure -6** of NIT Also, if the Tenderer is under Black List in any State / Central Government or other PSUs, then they need not apply. Tenderer shall submit Self-declaration as given in **Annexure -6** of NIT	

	<u>Acceptance of Technical Information as per Annexure -3 of tender uploaded</u> • Objective • Place of Work • Scope of Work • Detailed Description of Work • Product Specifications • Period of Contract / Warranty Support • Other Terms and Conditions • Subletting and transfer • Remuneration / Rates • Negotiation / Reverse Auction • MFL safety rules and regulation • Summary Termination • Laws Governing the Contract • Arbitration • Liquidated Damages • General Terms as per Tender	

TECHNICAL EVALUATION REPORT:

Description	Yes / No
WHETHER TECHNICALLY QUALIFIED	

COMMERCIAL EVALUATION SHEET

SNo.	Description	Yes / No
1	The quoted Price will be exclusive of all applicable taxes	
2	The vendor should provide Bank RTGS details	
3	Payment will be made only thru RTGS on expiry of 60 (for MSE's 45) days on confirmation of successful installation of all items with all aspects as per MFL Requirement and error free invoice subject to our acceptance. The tenderer shall neither be entitled to claim interest for the pending bills with MFL nor the delay in payment if any, give any right to tenderer to suspend the work under the contract.	
4	Security Deposit (SD) – 5% [Excluding GST] of the contract value	
5	Income Tax PAN Number	
6	Liquidated Damages Clause as per MFL Tender Point 17 of Annexure-3 of NIT	
7	Service Tax Registration proof to be attached	

COMMERCIAL EVALUATION REPORT:

Description	Yes / No
WHETHER COMMERCIALLY QUALIFIED	

ANNEXURE -5

Price Bid Break-up Format for Desktop and related components (Exclusive of taxes)

SNo	Product Description	Qty	Rate per Qty(₹)	Total Price(₹)
1	**Desktop Computers with accessories (As per Technical Specification Serial no 5.1)**	**100**		
2	**Anti-Virus INTERCEPT X ADVANCED (Managed by Sophos Central) (As per Technical Specification Serial no 5.2)**	**100**		
3	**Total charges exclusive of all applicable taxes for Serial NO 1 to 2**			

ANNEXURE – 6

INFORMATION ABOUT THE TENDERER

Sl. No.	Information Required	To be Filled in by Tenderer
1	Name of the Tenderer	
2	Address of Registered Office and Branches	
3	Address and Phone Number, Fax Number, Email ID etc.	
4	Composition of Tender (here state whether it is Hindu Joint Family Business, Proprietorship concern or Registered Partnership or a Limited Company)	
5	Nature of normal business of the tenderer	
6	Experience of similar working (Certificate to support statement must be enclosed)	
7	Any other experience and reference of the Companies (Attach separate sheet, if necessary). Copies of certificates (Award of contract and experience) to support statement must be attached.	
8	Details of Turnover	
9	Copy of PAN Card and 3 years IT Assessment order to be attached	
10	Three years audited statement of Accounts with Balance Sheet	
11	PF Code No.	
12	ESI Code No.	
13	Labour License No., if any.	
14	GST Registration No.	
15	Any court case is filed against you or your concern	
16	Have you / your Firm filed any case against MFL	

17	MSE's Details General SC/ST Women Entrepreneur	
	Category of the Firm – Under MSME (Enclose : Udyam Registration Certificate)	

Note: Copies of documents are required to be attached for Sl.No.5 to 14 and 17.

Incomplete information and non-submission of copies of supporting documents will lead to rejection of tender.

I/we declare that the above information is true to the best of my / our knowledge.

Place: **Signature of the Tenderer**

Date: **(Name & Office seal)**

SELF DECLARATION

I/We hereby declare that I/We have not been banned and de-listed / holiday listed by any Company / PSU / Government Department / Financial Institution / or having Litigation with MFL.

Place : **Signature of the Tenderer**

Date : **(Name & Office seal)**

ANNEXURE - 7

TENDERER UNDERTAKING

THE TENDERER HEREIN

- Agrees, accepts and abides by all the terms and conditions and covenants of the tender having read and understood the tender documents in full including the specification, scope of work, instructions, forms, annexures, terms and conditions etc

- Confirms and acknowledges that the bids placed by the tenderer are true, accurate & with the best knowledge of the tenderer

- Confirms that awarding of the contract/purchase order based on the bids of the tenderer is the sole discretion of MFL

- Undertakes to honour the bid(s), which is legally binding on, if the contract/purchase order is awarded to the tenderer

- Accepts the SD, LD & Penalty clauses and agrees to invocation of the respective clause(s) in case of non-fulfillment of commitment.

- Agrees to accept any changes, if any, to the tender that may be made subsequently after releasing the tender, but before the last date meant for submission of bids, with respect to specification, last date for bid submission and/or any other clauses/terms of the tender

Signature of the authorised person :

Name of the authorised person :

Designation of the authorised person :

Company's Seal :

ANNEXURE - 8

SECURITY DEPOSIT (SD) TERMS & CONDITIONS

The successful tenderer shall pay 5% of the total contract value (excluding GST) towards SD by Demand Draft or Insurance Surety Bond or Bank Guarantee in the approved format (Annexure-9) valid up to one year and a grace period of one year beyond the completion of the contract, issued by a Nationalized Bank or Scheduled Bank (not from Co-operative Bnak) to the satisfaction of MFL, payable and enforceable at Chennai or thru RTGS as per (Annexure-10), within 21 days from the date of intimation of his selection or before commencement of contract whichever is earlier. Independent confirmation of BG by the issuing Bank shall be sent directly to the DGM – MIS, Madras Fertilizers Ltd, Manali, Chennai - 600 068. The Bank Guarantee furnished towards the EMD amount is not adjustable towards security deposit and it will be returned to the contractor on furnishing security deposit payable by the tenderer, by way of DD or BG/RTGS. This should be submitted within 21 days from the date of intimation of his selection.

No interest shall be paid on the security deposit. Failure to pay the security deposit within 21 days from the date of award of contract or enter into contract shall be treated as failure to discharge the duties under the contract and shall result in cancellation of the offer of the contract. The EMD amount shall be forfeited and the tenderer shall be liable to compensate MFL for any losses incurred by MFL

The security deposit shall be refunded after 90 days from the date of completion of the contract subject to the contractor fulfilling all obligations/operations as required under the contract. Only after due satisfaction as regards to the payment of wages, bonus, ESI, Insurance & PF and Service Tax dues by the contractor, the security deposit will be refunded

MFL reserves the right to appropriate any part or the whole of the amount of the security deposit without prejudice to other claims against the contractor for losses suffered by MFL due to breach or failure on the part of the contractor or due to termination of contract or contractor becoming disqualified because of liquidation/insolvency or change of composition. The decision of MFL in respect of such losses, failures, breach, damages, charges, expenses or costs, shall be final and binding on the contractor and shall not be called into question

Whenever the security deposit falls short of the specified amount, consequent to any adjustment towards shortages/damages/losses, the contractor shall make good the deficit within 7 days from the date of receipt of intimation from the Company so that the total amount of security deposit shall not at any time be less than the specified amount

In the event of the security deposit being insufficient or if the security deposit has been wholly forfeited, the balance of the total sum recoverable from the contractor as the case may be, shall be deducted from any sum then due or which at any time thereafter may become due and payable to the contractor under this or any other contract with MFL. Should that sum also be not sufficient to cover the full amount recoverable, the contractor shall pay to MFL on demand the remaining balance due as a debit

ANNEXURE - 9

FORMAT FOR SD BG

(TO BE EXECUTED ON A NON-JUDICIAL STAMP PAPER OF APPROPRIATE VALUE)

To
Madras Fertilizers Limited

WHEREAS ……..
(name and address of the supplier) (hereinafter called "the supplier") has undertaken, in pursuance of contract no…… dated …… to supply (description of goods and services) (hereinafter called "the contract").

AND WHEREAS it has been stipulated by you in the said contract that the supplier shall furnish you with a bank guarantee by a Scheduled / Commercial Bank recognized by you for the sum specified therein as security for compliance with its obligations in accordance with the contract;

AND WHEREAS we have agreed to give the supplier such a bank guarantee;

NOW THEREFORE we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of …….. (amount of the guarantee in words and figures), and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of (amount of guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed thereunder or any of the contract documents which may be made between you and the supplier shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This guarantee shall be valid until the ……**.** With a claim revised up to……..

……..
(Signature of the authorized officer of the Bank)
……
Name and designation of the officer
……..
Seal, name & address of the Bank and address of the Branch

ANNEXURE - 10

MFL'S BANK ACCOUNT DETAILS FOR SUBMISSION OF SD THRU RTGS

1076

MANDATE FORM
Electronic Clearing Service (Credit Clearing) / Real Time Gross Settlement (RTGS)
Facility for receiving payments

A. Details of Accounts Holders :-

Name of Account Holder	MADRAS FERTILIZERS LIMITED
Complete Contact Address	MANALI, CHENNAI – 600 068
Telephone Number / Fax / Email	9884172251 / ins@madrasfert.co.in

B. Bank Accounts Details :-

Bank Name	STATE BANK OF INDIA
Branch Name with Complete Address, Telephone No. and Email	COMMERCIAL BRANCH 232, NSC BOSE ROAD, CHENNAI – 600 001
Whether the Branch is computerized?	YES
Whether the Branch is RTGS enabled? If yes then what is the Branch's IFSC Code	SBIN0007347
Is the Branch also NEFT enabled?	YES
Type of Bank Account (SB / Current / Cash Credit)	CC ACCOUNT
Complete Bank Account No. (Latest)	10242276424
MICR Code of Bank	600002014

Date of effect :-

I hereby declare that the particulars given above are correct and complete. If the transaction is delayed or not effected at all for reasons of incomplete or incorrect information. I would not hold the use Institution responsible. I have read the option invitation letter and agree to discharge responsibility expected of me as a participant under the Scheme.

Date : 11-09-2015

V. 11/09/2015
Authorised Signatory
V. MURALIDHARAN
General Manager - Finance & Accounts
MADRAS FERTILIZERS LIMITED
Manali, Chennai - 600 068

Certified that the particulars furnished above are correct as per our records.

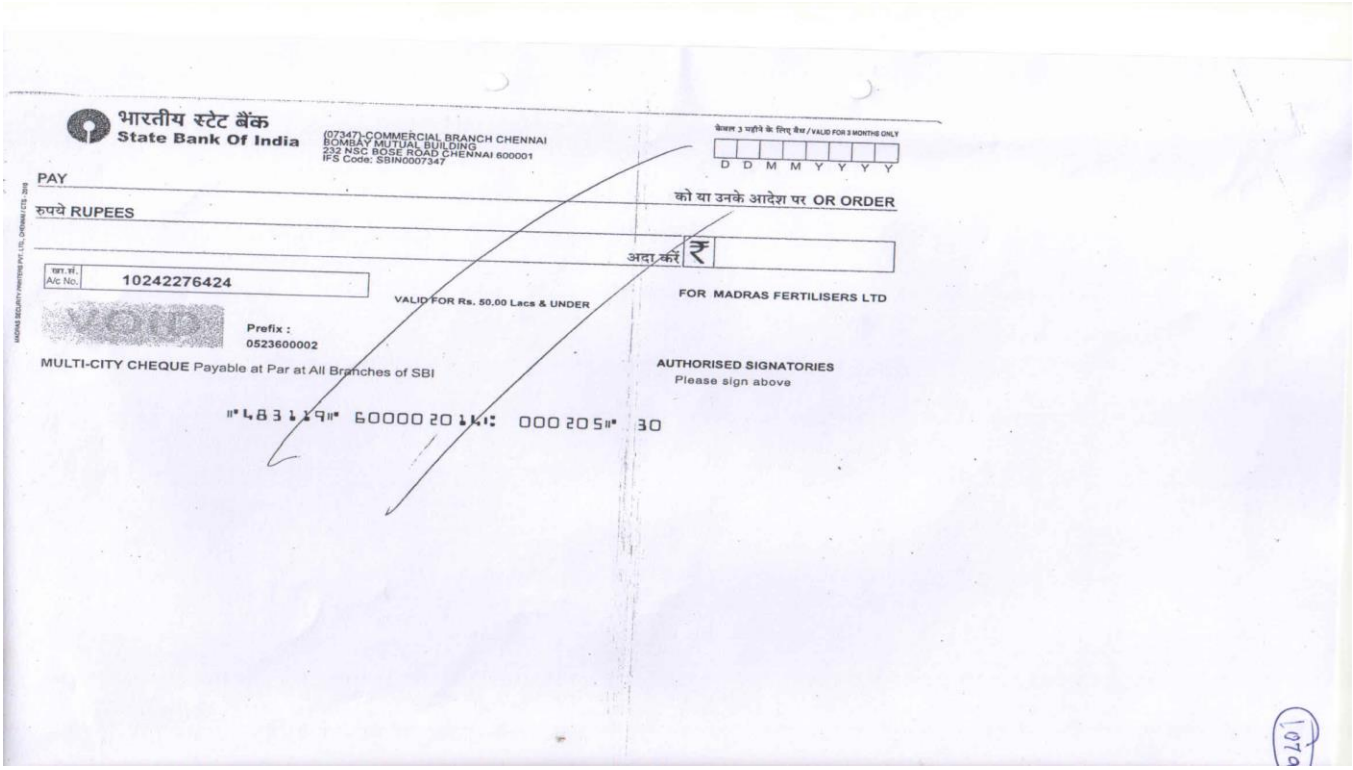
कृते भारतीय स्टेट बैंक
For STATE BANK OF INDIA

(Bank's Stamp)

Date : 11-09-2015

सहा. महाप्रबंधक / Assistant General Manager
Signature of the Bankers
वाणिज्यिक शाखा, चेन्नै / Commercial Branch, Chennai-1

1. Please attach a photocopy of cheque along with the verification obtained from the bank.
2. In case your Bank Branch is presently not "RTGS enabled", then upon its up-gradation to "RGTS Enabled" branch, please submit the information again in the above proforma to the Department at earliest.



भारतीय स्टेट बैंक
State Bank Of India

(07347)-COMMERCIAL BRANCH CHENNAI
BOMBAY MUTUAL BUILDING
232 NSC BOSE ROAD CHENNAI 600001
IFS Code: SBIN0007347

केवल 3 महीने के लिए वैध / VALID FOR 3 MONTHS ONLY
D D M M Y Y Y Y

PAY

रुपये RUPEES

को या उनके आदेश पर OR ORDER

अदा करें ₹

खा.सं. A/c No. 10242276424

VALID FOR Rs. 50,00 Lacs & UNDER

FOR MADRAS FERTILISERS LTD

VOID

Prefix :
0523600002

MULTI-CITY CHEQUE Payable at Par at All Branches of SBI

AUTHORISED SIGNATORIES
Please sign above

⑈483119⑈ 600002014⑆ 000205⑈ 30

ANNEXURE - 11

MADRAS FERTILIZERS LIMITED

BANK DETAILS & AUTHORISATION FOR RTGS/NEFT PAYMENT

REQUIRED DETAILS	TO BE FURNISHED BY THE VENDOR			
VENDOR NAME				
ADDRESS				
TELEPHONE NO.		FAX No.		
EMAIL ID				
CONTACT PERSONS'S NAME		Designation :		
MOBILE NO.				
EMAIL ID				
COMPANY'S PAN NO.				
IMPORT EXPORT CODE				
BANK ACCOUNT NO.				
VENDOR'S BANK NAME				
BANK ADDRESS / PHONE NO.				
VENDOR'S BANK CODE (MICR) NO.		GRPT CODE		
VENDOR'S BANK ACCOUNT NO.		NEFT CODE		
		RTGS CODE		
BANK SWIFT CODE (For foreign vendors)				
	Type of Account	Saving Acct / Current Acct. (Strike out which is not applicable)		
ARE YOU A	Manufacturer YES / NO	Dealer-YES / NO	Agent YES / NO	
CATEGORY OF THE FIRM	A. Micro	B. Small	C.Medium	
REGISTERED WITH	CST No.	SSI No.	EC No.	TIN No.

We hereby authorize Madras fertilizers Limited to make all the payments due to us with respect to above referred Enquiry through RTGS/NEFT Transfer

Place: Signature of Authorised Signatory:

Date: Name:

SEAL: Designation: (To be filled by MFL in case of ordering)

MFL Purchase Order No.	

RTGS-Real Time Gross Settlement Code NEFT-National Electronic Funds
IFSC- Indian Financial System Code

ANNEXURE - 12

M & D - Regional Office Address / Telephone / E-mail ID's

Sl.No	Address	Phone / FAX / E-mail ID	CM /RM & his Contact Nos.
1	**TRICHY** Door No.18, First Floor Alamelumangai Street Jeya Nagar, KK Nagar Post Trichy - 620 021	Phone : 0431 - 7969758 E-mail :mflrotry@gmail.com	S Durai Pandian, CM Mob:9994335477
2	**SALEM** 246/2, Ist Floor, Karkanar St, Five Roads, Salem – 636 004.	Phone : 0427 - 2443900 E-mail : mflroslm@gmail.com	P.Kumaresan, RM Mob: 9894612454
3	**MADURAI** 2/256, Rengasamy Street 2nd Main Road Gomathipuram Madurai – 625 020	Phone : 0452 - 3556707 E-mail : mflmduown@gmail.com	S.Durai Pandian, RM Mob: 9994335477
4	**VELLORE** 29, I Floor, 7th East Main Road, Gandhi Road Vellore - 632 006	Phone :0416-2249569 E-mail : mflrovel@gmail.com	S. Gouthaman, RM Mob: 9994385053
5	**HYDERABAD (TELANGANA)** D.No.11-5-338, Bazarghat Road. Redhills, Lakdi-ka-pul Hyderabad - 500 004	Phone : 040-23316155 E-mail : mflrohyd@gmail.com	N.Uma Shankar, CM Mob:9390163001
6	**VIJAYAWADA** Door No. 5-56-8, Flat No. S3 Lakshmi Apartments Ramineni Street,Patamata Vijayawada - 520 010	Phone : 0866-2973014 E-mail : mflrovja@gmail.com	N.Uma Shankar, CM Mob:9390163001
7	**KADAPA** Door No. 2/258, 1st floor Balaji Nagar Kadapa – 516 003	Phone : 08562-244897/244708 E-mail : mflrocdp@gmail.com	K. Athinarayanaswamy, RM Mob:9944147755
8	**BANGALORE** 66, "OMKAR" 1st floor 1st Block, 3rd Cross, 4th Main Banashankari 3rd Stage Bangalore - 560 085	Phone : 080-29742529 E-mail : mflroblr@gmail.com	S. Gouthaman, RM Mob: 9994385053
9	**DAVANGERE** 342/2, I Floor, Srinivasa Complex, II Main Road, Near Stadium, PJ Extension Davanagere – 577 004	Phone : 08192 – 256074 E-mail : mflrodvg@gmail.com	D.S. Deshpande, RM Mob: 9886011102
10	**BELLARY** Srilakshmi Venkateswara Nilaya No.3, Ward No.25, II Cross Shastri Nagar Bellary - 583 101	Phone : 08392 – 268248 E-mail : mflrobly@gmail.com	D.S. Deshpande, RM Mob: 9886011102
11	**COCHIN** A6, Bhaskar Apartments Narayanan Asan Road Ponnurunni, Vyttila Ernakulam	Phone : 0484-2349607/ 2339607 E-mail : mflrochn@gmail.com	D.Srinivasan, RM Mob:9447432141
12	**NEW DELHI** Flat No C-43, Ground Floor, Green Park Main, New Delhi 110016.	Phone : +91 98181 44273 +91 79043 07177	Sandeep Dugal Deputy Manager - Liasion Mob:98100 77986

ANNEXURE – 13

Preference to Make in India & Rule 144 (XI) of the General Financial Rules (GFRs), 2017 Clauses

S.n	Clause	Subject
1	Preference Make in India	This Tender is governed by Circular No. P-45021/2/2017-B.E.-II dated 15.06.2017, 28.05.2018, 29.05.2019, 20.06.2020 & 16.09.2020 issued by Govt. of India. "For this procurement, Public Procurement (Preference to Make in India), Order 2017 dated 15.06.2017, 28.05.2018, 29.05.2019 & 20.06.2020 and subsequent Orders issued by the respective Nodal Ministry shall be applicable even if issued after issue of this NIT but before finalization of contract/ POI WO against this NIT. In the event of any Nodal Ministry prescribing higher or lower percentage of purchase preference and/ or local content in respect of this procurement, same shall be applicable." Preference to Make in India including counter offering will be as per the Public Procurement (Preference to Make in India), Order 2017 available in the following links: https://dipp.gov.in/public-procurements https://dipp.gov.in/sites/default/files/PPP-MII-ORDER-2017_15062018_0.pdf https://dipp.gov.in/sites/default/files/Revised-PPP-MII-Order-2017_28052018.pdf https://dipp.gov.in/sites/default/files/PPP-MII%20Order%20dt%2029th%20May%2019_0.pdf https://dipp.gov.in/sites/default/files/PPP%20MII%20Order%20dated%204th%20June%_202020.pdf https://dipp.gov.in/sites/default/files/PPP%20MII%20Order%20dated%2016%2009%202020.pdf Certification (as applicable) giving the percentage of local content, in line with PPP-MII order, to be submitted as per attached Annexure-A. The onus of submission of appropriately certified documents lies with the bidder and MFL shall not have any liability to verify the contents and will not be responsible for the same. However, in case MFL has any reason to doubt the authenticity of the Local Content, MFL reserves the right to obtain the complete back up calculations before award of contract failing which the bid shall be rejected.

Attention is invited to Order (Public Procurement No.1) issued vide F.6/18/2019- PPD dated 23.07.2020, Order (Public Procurement No. 2) issued vide F.6/18/2019-PPD dated 23.07.2020, Order (Public Procurement No. 3) issued vide F.6/18/2019-PPD dated 24.07.2020, Office Memorandum (OM) No. F.18/37/2020-PPD dated 08.02.2021, OM No. F.12/1/2021-PPD(Pt.) dated 02.03.2021 and OM No. F.7/10/2021-PPD dated 08.06.2021. In this regard, the following is hereby ordered under Rule 144(xi) (as amended vide OM No. F.7/10/2021-PPD dated 23.02.2023) on the grounds stated therein, in supersession to all of the above mentioned Orders/ clarifications:

S.no	Clause	Subject
2	As mentioned above	I. Any bidder from a country which shares a land border with India will be eligible to bid in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) only if the bidder is registered with the Competent Authority. Further, any bidder (including bidder from India) having specified Transfer of Technology (ToT) arrangement with an entity from a country which shares a land border with India, shall also require to be registered with the same competent authority. II. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process. . "Bidder (or entity) from a country which shares a land border with India" for the purpose of this Order means: - a. An entity incorporated, established or registered in such a country; or b. A subsidiary of an entity incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established orregistered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or jointventure falls under any of the above IV. The beneficial owner for the purpose of (iii) above will be as under: 1. In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means. Explanation— a. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company; b. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

		2. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership; 3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals; 4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official; 5. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership. V. An Agent is a person employed to do any act for another, or to represent another in dealings with third person. VI. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority. VII. The registration shall be valid at the time of submission of bid and at the time of acceptance of bid. VIII. If the bidder was validly registered at the time of acceptance / placement of order, registration shall not be a relevant consideration during contract execution The above clause is not applicable to the bidders from those countries (even if sharing a land border with India) to which the GoI has extended lines of credit or in which the GoI is engaged in development projects. List of countries to which lines of credit have been extended or in which development projects are undertaken are available on the Ministry of External affairs website https:// www.mea .gov.in/ Compliance to Government of India order OM No.6/18/2019-PPD dated 23.07.2020 regarding restrictions under Rule 144 (XI) of the General Financial Rules (GFRs), 2017 to be submitted on the bidder's letterhead as per Annexure-(B) or Annexure-(C) - as applicable.

"I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; I certify that this bidder is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfills all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]"

Signature and Seal of the Company

Annexure -(A)

Declaration to be issued on Company letter head

In line with Government Public Procurement Order (Preference to Make in India) Order (PPP-MII Order), 2017 vide No. P-45021/2/2017-PP (BE-II) dated 04.06.2020, issued by DPIIT, Ministry of Commerce and Industry, we hereby certify that we, ... (Bidder name) are

a) 'Class-I local supplier' meeting requirement of local content equal to or more than50%,

b) 'Class-II local supplier' meeting requirement of local content more than 20% but less than50%,

(Strike off whichever is not applicable)

As defined under above referred Order for the following Item Sl Nos of MFL Tender No : _____ Dated

- Tender Item No./(s)-

Details of location at which local value addition will be made is asfollows:

.....
.....

By issuing this declaration, we understand and are in acceptance to the following-

- False declarations will be in breach of the Code of Integrity under Rule 175(1) (i) (h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law.
- In case of debarment by any procuring entity for violation of the provisions of the Public Procurement (Preference to Make in India), Order 2017 we shall not be eligible for preference for procurement by any other procuring entity for the duration of the debarment. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities, the debarment takes effect prospectively from the date of uploading on the website(s) of The Department of Expenditure, GOI in such a manner that ongoing procurements are not disrupted.
- We undertake the onus of responsibility of submission of appropriately certified documents. We understand that MFL is not at liability to verify the contents and will not be responsible for the declaration made by us. However, in case MFL has any reason to doubt the authenticity of the local content, MFL reserves the right to obtain the complete back up calculations before award of contract and we are liable to submit the same if requested by MFL. We also understand that our bid is liable for rejection in case we fail to submit the details as requested by MFL.

Seal and Signature of authorized signatory

Special Note-

In cases of procurement for a value in excess of Rs. 10 crores, the local supplier shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

* * *

Annexure-(B)

(Compliance to be submitted on the Bidder's Letterhead)
(as applicable)

Sub: Compliance to Government of India order OM No.6/18/2019-PPD dated 23.07.2020 regarding restrictions under Rule 144 (XI) of the General Financial Rules (GFRs), 2017

Tender Name :

Tender No. :

Project / Description :

We M/s (name of the bidder company) have read the clauses pertaining to Department of Expenditure's (DoE) Public Procurement Division Order (Public procurement no 1, 2 & 3 vide ref. F.No.6/18/2019-PPD dated 23.07.2020) regarding restrictions on procurement from a bidder of a country which shares a land border with India.

We hereby certify that we are not from such a country and eligible to be considered for this tender. (Note: Non-compliance of above said GoI Order and its subsequent amendment, (if any), by any bidder(s) shall lead for commercial rejection of their bids by MFL)

For and behalf of (Name of the bidder)

(Signature, date & seal of authorized representative of the bidder)

* * *

Annexure-(C)

(Compliance to be submitted on the Bidder's Letterhead)
(as applicable)

Sub: Compliance to Government of India order OM No.6/18/2019-PPD dated 23.07.2020 & regarding restrictions under Rule 144(XI) of the General Financial Rules (GFRs), 2017

Tender Name :

Tender No. :

Project / Description :

We M/s_____(name of the bidder company) have read the clauses pertaining to Department of Expenditure's (DoE) Public Procurement Division Order (Public procurement no 1, 2 & 3 vide ref. F.No.6/18/2019-PPD dated 23.07.2020) regarding restrictions on procurement from a bidder of a country which shares a land border with India.

We are from such a country which shares a land border with India & have been registered with the Competent Authority as specified in above said order. We hereby certify that we fulfill all requirements in this regard and are eligible to be considered.

Evidence of valid registration by the Competent Authority is attached.

(Note: Non-compliance of above said GoI Order and its subsequent amendment, (if any), by any bidder(s) shall lead for commercial rejection of their bids by MFL).

For and behalf of_____(Name of the bidder)

(Signature, date & seal of authorized representative of the bidder)

* * *

ANNEXURE – 14

EARNEST MONEY DEPOSIT (EMD) TERMS & CONDITIONS

1. The tenderer shall submit the Earnest Money Deposit of ₹1,00,000/- by way of demand draft drawn in favour of "Madras Fertilizers Limited" payable at Chennai or Bank Guarantee (BG) in the MFL approved format **(Annexure-15)** valid for **165 days** from the date of bid opening including 45 days claim period or thru RTGS as per details provided in **(Annexure – 10)**.

2. The independent confirmation of (DD/BG/e-BG/Insurance surety bond) by issuing Bank shall be sent directly to the DGM MIS, Madras Fertilizers Ltd., Manali, Chennai 600 068 with clear superscription of the tender number on the cover as **"EMD for - TENDER No: ESER/MIS/ MIS-DESKTOP/150424/002 dated 15/03/0024 on before 17.04.2024**

3. The tenderer is not entitled for any interest on the Earnest Money Deposit and not for any right of award of contract

4. Tenders not accompanied by EMD shall summarily be rejected

5. After submission of

6. 5% of the contract value as security deposit by way of DD/BG or through RTGS by the successful tenderer, EMD submitted by way of BG will be returned to them. EMD will be refunded to the successful tenderer only after receipt of Security Deposit.

7. The EMD amount shall be forfeited without prejudice to any other claim, if the tenderer, after submitting his tender, resiles from his offer or modifies the terms and conditions thereof or fails to enter into agreement and take up the work within 21 days from the date of award of the contract

8. Unreturned EMD in respect of earlier tenders, if any, cannot be adjusted against this tender.

9. **Return of EMD:** The EMD shall be returned to unsuccessful tenderers after finalization of tender. The EMD refund (if paid thru DD/RTGS) shall be made to unsuccessful bidders thru E-payment. Hence, Bank Details as per attached format **(Annexure –11)** to be furnished with Banker's Certificate. In the case of BG, it will be returned to unsuccessful tenderers after finalization of the contract

10. The details of the Earnest Money Deposit document should be submitted physically to the Department within three working days from the date of opening the tender and the scanned copy should be furnished at the time of bid submission online. They should be same otherwise the tender will be summarily rejected.

ANNEXURE - 15

FORMAT FOR BANK GUARANTEE FOR FURNISHING EMD

(TO BE EXECUTED ON A NON-JUDICIAL STAMP PAPER OF APPROPRIATE VALUE)

To
Madras Fertilizers Limited

(TO BE EXECUTED ON A NON-JUDICIAL STAMP PAPER OF APPROPRIATE VALUE)

Whereas ……
(hereinafter called the "tenderer")
has submitted their offer dated …… for the supply of …… (hereinafter called the "tender") against the purchaser's tender enquiry No…… …… KNOW ALL MEN by these presents that WE …… ……..... of …… having our registered office at ……are bound unto MFL (hereinafter called the "Purchaser")in the sum of…… for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ……. day of …… 20 ……

THE CONDITIONS OF THIS OBLIGATION ARE:

(1) If the tenderer withdraws or amends, impairs or derogates from the tender in any respect within the period of validity of this tender.

(2) If the tenderer having been notified of the acceptance of his tender by the Purchaser during the period of its validity:-
   a) If the tenderer fails to furnish the Performance Security for the due performance of the contract.
   b) Fails or refuses to accept / execute the contract.

WE undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force upto and beyond 45 days after the period of tender validity and with a claim period of one year from the date of validity period of Bank guarantee and any demand in respect thereof should reach the Bank not later than the above date.

……
(Signature of the authorized officer of the Bank)
……
Name and designation of the officer
……
Seal, name & address of the Bank and address of the Branch