The Oriental Insurance Company Limited

Head Office, New Delhi

Corrigendum 1

For

Selection of Vendor for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution

(Tender Reference No.: OICL/HO/ITD/DITSM/2022/01 dated 09/12/2022)

Corrigendum dated 09/01/2023

Information Technology Department

The Oriental Insurance Company Limited
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

CIN- U66010DL1947GOI007158
www.orientalinsurance.org.in

1. Introduction

OICL has published the RFP vide Tender Reference No.: OICL/HO/ITD/DITSM/2022/01 dated 09/12/2022 for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution

Following changes have been made in the above stated RFP. All other terms and conditions of the RFP shall remain unchanged. Please treat this Corrigendum as an integral part of the RFP documents issued.

Corrigendum

In reference to the aforesaid RFP, all are advised to note the following:

2. Modification in RFP Clauses

#	RFP Clause Reference	RFP Clause	Revised Clause
1	1.7: Project Timelines	Anti-Virus with EDR T+2 months	Anti-Virus with EDR T+3 months
2	2. Scope of Work Upgrade of Active Directory	The Bidder shall be responsible for User, Machine (Laptop/Desktop) & User Migration to new Active Directory Domain from the existing Domains without any disruption in day-to-day work.	The Bidder shall be responsible for User, Machine (Laptop/Desktop) & User Updation to updated Active Directory Domain from the existing Domains without any disruption in day-to-day work
3	2. Scope of Work Anti Virus	Addition	Bidder to note that the tentative date for closure of evaluation of the RFP is February- March'23 Bidder to ensure that adequate licenses & support from existing AV OEM is factored in the RFP till operationalization of the new AV EDR Solution. Bidder to ensure seamless migration from existing AV to new proposed AV EDR Solution ensuring that there is no gap in support during migration from existing AV to new AV EDR Solution.
4	Appendix 1: Technical Specifications Anti-Virus with EDR	Entire Sheet	Please Refer Section 3 for Revised Specifications for Anti-Virus & EDR EDR
5	Appendix 1: Technical Specifications EMS; Pt.22	The proposed solution should have the capability to monitor both user and system initiated network traffic between client machines and servers and between servers, collecting network and server performance and availability	Clause stands deleted

#	RFP Clause Reference	RFP Clause	Revised Clause
		data in real time, thus enabling administrators to pinpoint the cause of delays and quantify the business impact of detected performance issues related to end users	
6	Appendix 1: Technical Specifications EMS; Pt.33	The modules/products should be from a single product family/suite so as to ensure the integration and high level of data exchange between various layers.	The modules/products should be from COTS OEM so as to ensure the integration and high level of data exchange between various layers.
7	Appendix 1: Technical Specifications EMS; Pt.48	The tool should be able to measure and collect data from, and set service level reporting on ICMP echo (ping), SNMP MIB variable, services like HTTP, if required. Alerts should be available when the SLA is violated	Clause stands deleted
8	Appendix 1: Technical Specifications EMS; Pt.54	The product should be scalable. It should support data collectors distributed across locations on collect systems, which should be able to gather and measure statistics from the IT infrastructure if required. Distributed data collection and measurement	Clause stands deleted
9	Appendix 1: Technical Specifications EMS; Pt.87	Should provide a web-based management dashboard for visibility into ITIL incident management and problem management data. Includes out-of-the-box reports, such as MTTR trending, cumulative return on investment (ROI), most frequent resolution workflow, and incident and alert trending correlated to ITIL configuration items. Users should be allowed to create custom reports.	Clause stands deleted
10	Appendix 1: Technical Specifications Helpdesk Solution ; Pt.1.1	The proposed IT Service Management solution should be built on ITIL framework and must be officially certified on the current ITIL v4 best practices on at least 10 processes by Pink Elephant. The ITIL4 processes that are relevant and needs to be assessed to meet the minimum functional criteria are Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management. The certification copy to be submitted along with the formal technical response.	The proposed IT Service Management solution should be built on ITIL framework and must be officially certified on ITIL best practices on at least 3 processes by Pink Elephant. (The processes that are relevant and needs to be assessed to meet the minimum functional criteria are Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management.

#	RFP Clause Reference	RFP Clause	Revised Clause
11	Appendix 1: Technical Specifications Helpdesk Solution ; Pt.7.4	Upon submission, every request should be assigned with unique-id which shall remain unique throughout the lifecycle and the request id should not be re-used. It should be possible to customize the numbering format of the generated request (ex: date-month-branch ID - type of asset - xxx)	Clause stands deleted
12	Appendix 1: Technical Specifications Helpdesk Solution ; Pt.8	Engineer Availability / Attendance tracking - System should provide a facility to track engineer's attendance and availability for taking up the call. - Helpdesk should have a facility to check the availability of engineer(online) before assigning a call to avoid SLA breaches.	Clause stands deleted
13	Appendix 1: Technical Specifications Helpdesk Solution ; Asset Discovery, Pt.3	Discovery system should have the ability to capture configuration files for the purposes of comparison and change tracking.	Discovery system should have the ability to capture configuration changes for the purposes of comparison and change tracking.
14	Bill of Material	Addition Other Costs	Particulars: Additional License of Existing AV till new AV EDR Solution is operational & implemented Qty. 13000

3. Specifications for Anti-Virus & EDR

#	Anti Virus & Anti-Malware	Compliance (Yes/No)	Remarks
	General		
1	The proposed solution should be purpose build, unified agent for AV features with on-premise architecture		
2	The proposed solution shall be licensed for at least 10,000 client machines		
3	The proposed solution client shall be loaded on the endpoints and the server shall distribute the updates to the clients		
4	The proposed solution shall provide a Central Management dashboard to manage the solution		
5	The solution must have the ability to generate visual reports. Solution must provide agent health status		
6	Solution must provide central management functions in terms of logs, threat intelligence, status of managed products/devices		

#	Anti Virus & Anti-Malware	Compliance (Yes/No)	Remarks
7	Central management should work as centralized threat sharing/management server with the managed clients		
8	Solution should be able to provide a central view of threat detections for managed devices		
9	Solution should be able to generate downloadable reports from existing and customizable templates		
10	The proposed solution should be deployed in centralized architecture to manage policies and should be controlled centrally.		
11	The solution should support the Windows OS which will be under active support from Microsoft during the duration of this contract. Currently OICL is using the following Operating Systems Platforms- Windows 8.1, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest.		
12	The proposed solution should have the following protection mechanism: 1.Anti-Malware, anti-ransomware protection 2. Host Intrusion Prevention System / Anti exploit module 3. Application Control 4. Zero/Anti Phishing & end point compliance		
13	The proposed solution shall offer all the features specified herein in a single unified installation. Installation of multiple agents to achieve the requirement is not acceptable.		
14	The proposed solution should potentially block the endpoint system from loading physical devices on USB bus such as removable storage devices, Bluetooth, Wi-Fi network cards etc.		
15	The proposed solution shall provide logs of the device control feature to detect attempts of connecting unauthorized devices		
16	The proposed solution shall allow usage of authorized USB devices by users and blocking of unauthorized USB devices. The solution shall allow exclusion of authorized USB devices by using their vendor ID, product ID or serial number		
17	The proposed solution shall provide management of storage devices and allow restrictions on their usage to allow, Block or make the device Read- Only along with the option of providing exceptions		
18	The proposed solution shall provide following installation methods: 1. EXE/MSI Package based installer 2. Web based installation 3. Login script based installation 4. Remote installation 5. Through AD or through proposed EMS		

#	Anti Virus & Anti-Malware	Compliance (Yes/No)	Remarks
19	All the client components should be installed using the single client package Deployment tool if required, for end point rollout will be responsibility of bidder		
20	The proposed solution should prevent normal user from uninstalling the endpoint security client		
21	The proposed solution shall provide detection of endpoints that do not have the agent installed		
	Malware Protection		
22	The proposed solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits		
23	The proposed solution shall also protect against certain non-virus threats, such as Spyware, adware, dialers, joke programs, remote access and hacking tools, which can be used with malicious intent		
24	The solution will leverage multiple sensors to effectively and uniquely identify generic malware behaviors as well as malware family specific behaviors.		
25	The proposed solution should be able to do full scan of files / folders with a choice of specifying directories and file extensions not to be scanned		
26	The proposed solution should provide performance control while scanning files/folders/Hard disk		
27	The solution will identify and block out-going communication to malicious C&C sites. Cloud threat intelligence resources will be used for updates and identification of zero-day C&C attacks		
28	The proposed solution should provide behavioral analysis using machine learning and artificial intelligence to detect and mitigate emerging unknown security threats, which does not have any signatures		
29	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser		
30	The proposed solution shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed		
31	The proposed solution on detection of a malware infection, should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation console from centralized Management console:		
32	The proposed solution shall protect against fileless malware and shall utilize behavioral techniques to detect malware based on the behavior of the file: 1. Detected malicious file 2. Affected registry entries 3. any new files dropped by malware		

#	Anti Virus & Anti-Malware	Compliance (Yes/No)	Remarks
	4. Kills processes that Trojans create 5. Repairs system files that Trojans modify		
33	The proposed solution should have tamper protection against malware that attempt to disable security measures		
34	The proposed solution should store event data at endpoint client while it is disconnected from the corporate network and forwards it on reconnection		
35	The proposed solution shall provide detection and blocking of Command and Control (C&C) traffic and prevent access to malicious and dangerous websites		
36	The proposed solution must provide application enforcement actions based on malicious file types such as Delete, Quarantine		
	Anti-Exploit, Anti Ransomware Protection		
37	The proposed solution shall protect the endpoint against the exploitation of vulnerabilities in operating system and other applications		
38	The solution will protect against zero-day ransomware without requiring signature updates. The solution will remediate and restore files that were encrypted during a ransomware attack. Should have capability to identify and trace malicious ransomware payloads and PowerShell obfuscated code injections into memory & registry.		
39	The proposed solution shall provide ransomware protection against unauthorized encryption or modification		
40	The proposed solution must provide the flexibility to create firewall rules for controlling in bound and out bound rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users		
41	The solution will protect against existing and zero- day ransomware without requiring signature updates. The anti-ransomware capability should have auto rollback feature to restore the system back to original state.		
	Application Control		
42	The proposed solution provides a capability to create a allow or a deny policy to manage known and unknown applications, file types, and executables		
43	The proposed solution is able to provide a syncing mechanism with a reliable file reputation source and global usage details to allow cross checking of known bad/good files. This source must be constantly kept up- to-date with the latest known bad/good file listing		
44	The solution will be used to restrict access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes		
	Security Definition Updates		

#	Anti Virus & Anti-Malware	Compliance (Yes/No)	Remarks
45	The proposed solution OEM should have a 24/7 security service update and should support real time updates of the system on release		
46	The proposed solution shall have an updating mechanism using local update server		
47	The proposed solution shall allow for incremental update of definitions		
48	The proposed solution shall provide a mechanism for updates of roaming devices or clients which are connected to Internet		
	Management and Reporting		
49	The proposed solution shall offer enterprise-wide visibility over the status of all the deployed components. The dashboard shall provide a summarized view to analyze top threats & summary of malware traffic or any other threats		
50	The proposed solution shall provide hierarchical grouping of machines and policy deployment		
51	The proposed solution shale offer a central repository of the updates that can be distributed to the managed components		
52	The proposed solution should have minimum log retention period of upto 180 days		
53	The proposed solution shall be able to receive logs from the managed components and endpoints and store them centrally		
54	The proposed solution shall collect the events occurring on endpoints. The solution shall also provide the functionality to forward of these events to the SIEM.		
55	The proposed solution shall provide alerts to users in case of any security incident in case of any failure to clean		
56	The proposed solution must provide notifications for important events. The notifications must be send through email or SNMP traps		
57	The proposed solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components		
58	The proposed solution should be capable of providing detailed reports containing data from all the deployed components		
59	The proposed solution should allow exporting of reports to PDF or CSV formats		
	Anti-Malware Protection for Linux Operating System Environment		
60	The Selected bidder needs to provide anti-malware solution for 100 instances of Server RHEL/Suse/Cent OS. The quoted solution may be different product from the solution proposed for desktops and laptops.		

#	End Point Detection & Response	Compliance (Yes/No)	Remarks
	End Point Detection & Response (EDR Desktop & Laptops)		
1	The proposed solution should be purpose build, unified agent for EDR features with on-premise architecture. In case the proposed EDR solution is different from the proposed AV then both solutions are able to coexist with each other simultaneously without any interference.		
2	The proposed solution shall be licensed for at least 10,000 client machines		
3	The proposed solution should provide context- aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls		
4	The proposed solution should perform multi-level sweep across endpoints using rich-search criteria as mentioned below		
5	User-defined criteria like User Name, File - Name, File – Hash, IP address, Hostname, Registry Key, Registry Value Name & Registry Value Data		
6	The proposed solution should be able to create multi-stage detailed kill-chain for performing the root cause analysis of an incident. Cyber Kill chain should also provide reputation of the files from the global threat intelligence as well		
7	The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices. 1. Scan disk Files 2. Scan in memory process 3. Search registry		
8	The proposed solution to provide the advance response capabilities as mentioned below 1. Kill process 2. Isolate device remotely 3. Block process & Forensics Analysis with remediation.		
9	The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like domains, file-hashes and shall also allow blocking of the files/file- hashes/domains/URLs identified by the IOCs		
10	Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system		
11	Solution must provide a way to isolate a system that ensures preventative controls are preserved through reboots. Isolation settings must be present to allow endpoint to be isolated from threats but able to connect to investigation/remediation systems		

#	End Point Detection & Response	Compliance (Yes/No)	Remarks
12	Solution must continuously collect system events necessary for detection and analysis. Solution will create an incident analysis for every detection/prevention that occurs/anaylst conducts. This analysis should include process execution trees even across boots if relevant.		
13	Solution must continuously collect system events necessary for detection and analysis. The proposed solution must list specific items that are collected in real-time. Examples must include, but not limited to, process events, file & registry modifications, network connections, cross-process activity, command line arguments, windows events, DNS queries and responses		
14	The solution should showcase affected process, affected registry keys & affected files in OS environment		
15	The solution will showcase malicious file emulation screenshots in Sandbox environment. The solution must have Integration with SIEM		
	End Point APT and Sandbox Capibilities		
16	The solution must have capabilities to scan Incoming files and extract all potential malicious content such as scripts, macros and active content. The original file must be accessible by end user if is found to be benign/legitimate by the sandbox		
17	The solution should allow for forensics analysis and report of any indicator found through the EDR platform. Forensic report will automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack.		
18	All files written on the file-system will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined/block if found as malicious. SI to propose Anti-APT appliance for the dynamic analysis of unknown files.		
19	The proposed sandbox solution should be deployed in standalone mode at DC and DR		
20	The proposed sandbox solution should be a purpose built appliance with redundant power supplies		
21	The proposed sandbox solution should integrate with proposed EPP solution		
22	The solution must identify malware, including zero day exploits, polymorphic/ metamorphic payloads and obfuscated java-scripts.		
23	The solution should have the ability to analyze and detect malware in common file formats including (but not limited to) the following types: 1. Compressed archives – Zip, Rar 2. Common Text document Formats: MS Word formats (doc, docx), pdf 3. Common Spreadsheet formats: MS Excel formats (xls, xlsx) 4. Presentation formats: MS PowerPoint formats (ppt, pptx).		

#	End Point Detection & Response	Compliance (Yes/No)	Remarks
	5. Common Executable Formats: exe, dll, jar All the hardware & software licenses including the virtual machines required for analyzing above file types are in the scope of bidder.		
24	The virtual execution environment must not be detectable by malware in order to evade detection.		
25	The single appliance should be able to support upto 24 virtual instances in a single appliance.		
26	The solution must provide AI/ML based sandboxing for the detonation of the unknown threats. For the dynamic run time analysis the solution should be able to support following operating systems in the sandboxing environment - Win 8.1 ,Win 10 and latest Supported Windows platforms All the virtual instances should be licensed from day one.		
27	The solution should store the files submitted to the sandbox for further analysis.		
28	Multiple notification methods shall be supported like email and SNMP traps etc.		
29	Web/Client based Management shall be available for local administration.		
30	Notifications should be sent to administrators in case of warnings & critical events. All the attack incidents to be mapped with MITRE tactics for the standardize view of techniques used by attackers		