Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
1	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	We support windows operating systems which are under active windows support from Microsoft. As this contract is for 6 years and some of these OS will be going EOL from MS during that period the same will need to be upgraded to latest Win OS versions to keep continuing the AV support. We hope this is in line with OICL expectations.	Please refer Corrigendum for revised specifications
2	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Our solution support Windows and Mac OS. For RHEL and Cent OS which are server OS we request you to kindly remove the same as the technical specifications for server OS will differ from desktop/windows environment. The server solution will have a different product and functionalities suited to server environment. We request you to define server technical requirements separately.	Please refer Corrigendum for revised specifications
3	77	Technical Specifications; AV + EDR	1.11.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Application Control & Disk encryption	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
4	77	Technical Specifications; AV + EDR	1.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Zero Phishing & end point compliance	We understand OICL is looking for anti phishng capability. If so kindly modify to 'anti phishing'	Please refer Corrigendum for revised specifications
5	77	Technical Specifications; AV + EDR	1.11.3.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Web based installation	We wish to highlight that this feature is not supported if OICL is using Server Core installation for Windows, kindly clarify if server core is being used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
6	77	Technical Specifications; AV + EDR	1.11.3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Remote installation	Remote installation is not possible for Windows 8.1 (basic versions) and Windows 10 (Home Edition) kindly clarify if these OS versions are/will be used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications
7	79	Technical Specifications; AV + EDR	2.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as non-compliant and can apply restrictive policies to them.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
8	79	Technical Specifications; AV + EDR	2.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	windows services created by malware	Kindly modify to 'Kills processes that Trojans create'.	Please refer Corrigendum for revised specifications
9	79	Technical Specifications; AV + EDR	2.11.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	any other system settings affected by malware	Kindly modify 'Repairs system files that Trojans modify'.	Please refer Corrigendum for revised specifications
10	79	Technical Specifications; AV + EDR	2.17/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution must provide application of enforcement actions based on malicious file types such as Delete, Block, Quarantine	Kindly delete 'Block' as malicious file will either be deleted or quarantined.	Please refer Corrigendum for revised specifications
11	79	Technical Specifications; AV + EDR	2.18/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Preventive controls from advanced sophisticated attack against users including Anti Phishing, Web form protection, account takeover protection etc.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
12	79	Technical Specifications; AV + EDR	2.19/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation	Kindly modify 'Solution should be able to categorise phishing url using reputation engine.'	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
				based Techniques to identify phishing URL's :		
13	79	Technical Specifications; AV + EDR	2.20/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Full disk encryption - All volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
14	80	Technical Specifications; AV + EDR	3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will protect against existing and zeroday ransomware without requiring signature updates. The anti-ransomware capability should have auto rollback feature to restore the system back to original state. The anti-ransomware solution has third party-validation.	Kindly delete 'third party validation'.	Please refer Corrigendum for revised specifications
15	80	Technical Specifications; AV + EDR	3.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution should support zero trust policy for files downloaded from untrusted sources on web. Solution must sanitize all the active content / scripts from the file before it deliver to end user.	Kindly delete this clause as it is more of web security feature.	Please refer Corrigendum for revised specifications
16	80	Technical Specifications; AV + EDR	4.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should allow for selection of Native encryption or BitLocker Management via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
17	80	Technical Specifications; AV + EDR	4.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should support seamless switching between BitLocker Management and Native encryption via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
18	82	Technical Specifications; AV + EDR	7.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. (Data collected through post-event scripts or live interaction with host is covered in a separate requirement.) 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	Kindly delete '(Data collected through post-event scripts or live interaction with host is covered in a separate requirement.)'	Please refer Corrigendum for revised specifications
19	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 1.10	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Please refer Corrigendum for revised specifications
20	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 2.5	The proposed solution should provide performance control while scanning files/folders/Hard disk	The proposed solution should provide performance control/optimized scan while scanning files/folders/Hard disk **justification**- Change in language to have clarity on the use case.	Please refer Corrigendum for revised specifications
21	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications-2.8	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser and should support majority of browsers Chrome, Edge, Safari, Firefox, Brave **justification**- Solution should offer the comprehensive coverage for most complete security.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
22	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -8	Additional point: EDR	The solution must block the OICL user from using it's corporate credentials in a untrusted site that does not belong to corporate credential domain to secure the user identity and the credentials. Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's & leverage application of AI & ML to meet this requirement. **justification** - Use of stolen credentials is most used tactics by cyber criminals to get the initial access by Ransomware actors. As per Verizon data breach report Credentials & Phishing are top two path leading to your state a.k.a entry point for the Cyber criminals. ref- https://www.verizon.com/business/resources/reports/dbir/	Please refer Corrigendum for revised specifications
23	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.1	2.3.3 Antivirus Solution with EDR Functionality	We understand that End Point Protection security controls NGAV, EDR (Anti-Exploit, Anti Ransomware Protection) & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
24	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications	The proposed solution should be purpose build, unified agent for all features with on-premise architecture	We understand that End Point Protection security controls NGAV, EDR & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications
25	22	Scope of Work AV + EDR	2	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with Windows operating system for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with **Open Servers & Windows server/endpoint** for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	Please be guided by the RFP
26	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.11	The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response	Our understanding is that end point anti-apt sandboxing solution has to be natively integrated into EDR capabilities and all the required hardware to be factored for on-premise deployment. We request you to provide clarification in this regards and change the requirements The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response, Anti-APT	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
27	33	Payment Terms	3.1.9 Payment Terms	**Software** Delivery of respective software & its related components as per the actual supply (after due inspection) - 70% Successful completion of customization and successful acceptance of software by OICL (after due inspection)- 30%	**Software** Delivery of respective software & its related components as per the actual supply (after due inspection) - **90%** Successful completion of customization and successful acceptance of software by OICL (after due inspection)- **10%**	Please be guided by the RFP
28	33	Payment Terms	3.1.9 Payment Terms	**FM Manpower** Quarterly in arrears	**FM Manpower** **Quarterly in advance**	Please be guided by the RFP
29	52	Service Level	Penalties	OICL reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the payouts. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a maximum of 10% of the overall contract value.	OICL reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the payouts. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a **maximum of 5% of the overall contract value.**	Please be guided by the RFP
30	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	We support windows operating systems which are under active windows support from Microsoft. As this contract is for 6 years and some of these OS will be going EOL from MS during that period the same will need to be upgraded to latest Win OS versions to keep continuing the AV support. We hope this is inline with OICL expectations.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
31	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Our solution support Windows and Mac OS. For RHEL and Cent OS which are server OS we request you to kindly remove the same as the technical specifications for server OS will differ from desktop/windows environment. The server solution will have a different product and functionalities suited to server environment. We request you to define server technical requirements separately.	Please refer Corrigendum for revised specifications
32	77	Technical Specifications; AV + EDR	1.11.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Application Control & Disk encryption	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
33	77	Technical Specifications; AV + EDR	1.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Zero Phishing & end point compliance	We understand OICL is looking for anti phishng capability. If so kindly modify to 'anti phishing'	Please refer Corrigendum for revised specifications
34	77	Technical Specifications; AV + EDR	1.11.3.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Web based installation	We wish to highlight that this feature is not supported if OICL is using Server Core installation for Windows, kindly clarify if server core is being used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications
35	77	Technical Specifications; AV + EDR	1.11.3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Remote installation	Remote installation is not possible for Windows 8.1 (basic versions) and Windows 10 (Home Edition) kindly clarify if these OS versions are/will be used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
36	79	Technical Specifications; AV + EDR	2.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as non-compliant and can apply restrictive policies to them.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
37	79	Technical Specifications; AV + EDR	2.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	windows services created by malware	Kindly modify to 'Kills processes that Trojans create'.	Please refer Corrigendum for revised specifications
38	79	Technical Specifications; AV + EDR	2.11.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	any other system settings affected by malware	Kindly modify 'Repairs system files that Trojans modify'.	Please refer Corrigendum for revised specifications
39	79	Technical Specifications; AV + EDR	2.17/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution must provide application of enforcement actions based on malicious file types such as Delete, Block, Quarantine	Kindly delete 'Block' as malicious file will either be deleted or quarantined.	Please refer Corrigendum for revised specifications
40	79	Technical Specifications; AV + EDR	2.18/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Preventive controls from advanced sophisticated attack against users including Anti Phishing, Web form protection, account takeover protection etc.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
41	79	Technical Specifications; AV + EDR	2.19/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's :	Kindly modify 'Solution should be able to categorise phishing url using reputation engine.'	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
42	79	Technical Specifications; AV + EDR	2.20/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Full disk encryption - All volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
43	80	Technical Specifications; AV + EDR	3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will protect against existing and zeroday ransomware without requiring signature updates. The anti-ransomware capability should have auto rollback feature to restore the system back to original state. The anti-ransomware solution has third party-validation.	Kindly delete 'third party validation'.	Please refer Corrigendum for revised specifications
44	80	Technical Specifications; AV + EDR	3.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution should support zero trust policy for files downloaded from untrusted sources on web. Solution must sanitize all the active content / scripts from the file before it deliver to end user.	Kindly delete this clause as it is more of web security feature.	Please refer Corrigendum for revised specifications
45	80	Technical Specifications; AV + EDR	4.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should allow for selection of Native encryption or BitLocker Management via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
46	80	Technical Specifications; AV + EDR	4.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should support seamless switching between BitLocker Management and Native encryption via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
47	82	Technical Specifications; AV + EDR	7.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. (Data collected through post-event scripts or live interaction with host is covered in a separate requirement.) 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	Kindly delete '(Data collected through post-event scripts or live interaction with host is covered in a separate requirement.)'	Please refer Corrigendum for revised specifications
48	33	Payment Terms	3.1.9 Payment Terms	**Software** Delivery of respective software & its related components as per the actual supply (after due inspection) - 70% Successful completion of customization and successful acceptance of software by OICL (after due inspection)- 30%	**Software** Delivery of respective software & its related components as per the actual supply (after due inspection) - **90%** Successful completion of customization and successful acceptance of software by OICL (after due inspection)- **10%**	Please be guided by the RFP
49	33	Payment Terms	3.1.9 Payment Terms	**FM Manpower** Quarterly in arrears	**FM Manpower** **Quarterly in advance**	Please be guided by the RFP
50	52	Service Level	Penalties	OICL reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the payouts. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a maximum of 10% of the overall contract value.	OICL reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the payouts. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a **maximum of 5% of the overall contract value.**	Please be guided by the RFP
51	21	Scope of Work AD		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	need clarity	Revised clause reads: "The Bidder shall be responsible for User, Machine (Laptop/Desktop) & User Updation to updated Active Directory Domain from the

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
						existing Domains without any disruption in day-to-day work"
52	21	Scope of Work AD		As per this tender we need to upgrade domain from 2012 r2 to latest. How the above point no 8 come into scope where no new Active Directory domain is created	need clarity	Please refer Corrigendum for revised clause Revised clause reads: "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"
53	21	Scope of Work AD		Which tool we are going to use for monitoring and sending AD Health Report daily.	need clarity	Bidder to propose Enterprise Management Solution to cater to the said requirement
54	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 1.1	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Please refer Corrigendum for revised specifications
55	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 2.5	The proposed solution should provide performance control while scanning files/folders/Hard disk	The proposed solution should provide performance control/optimized scan while scanning files/folders/Hard disk **justification**- Change in language to have clarity on the use case.	Please refer Corrigendum for revised specifications
56	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications-2.8	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser and should support majority of browsers Chrome, Edge, Safari, Firefox, Brave **justification**- Solution should offer the comprehensive coverage for most complete security.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
57	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -8	Additional point: EDR	The solution must block the OICL user from using it's corporate credentials in a untrusted site that does not belong to corporate credential domain to secure the user identity and the credentials. Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's & leverage application of AI & ML to meet this requirement. **justification** - Use of stolen credentials is most used tactics by cyber criminals to get the initial access by Ransomware actors. As per Verizon data breach report Credentials & Phishing are top two path leading to your state a.k.a entry point for the Cyber criminals. ref- https://www.verizon.com/business/resources/reports/dbir/	Please refer Corrigendum for revised specifications
58	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.1	2.3.3 Antivirus Solution with EDR Functionality	We understand that End Point Protection security controls NGAV, EDR (Anti-Exploit, Anti Ransomware Protection) & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
59	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications	The proposed solution should be purpose build, unified agent for all features with on-premise architecture	We understand that End Point Protection security controls NGAV, EDR & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications
60	22	Scope of Work AV + EDR	2	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with Windows operating system for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with **Open Servers & Windows server/endpoint** for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	Please be guided by the RFP
61	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.11	The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response	Our understanding is that end point anti-apt sandboxing solution has to be natively integrated into EDR capabilities and all the required hardware to be factored for on-premise deployment. We request you to provide clarification in this regards and change the requirements The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response, Anti-APT	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
62	19	Scope of Work	Bandwidth Details	The following table specifies the bandwidth available at various OICL offices:	Please specify the distribution of endpoints at each location (RO, DO, BO,EC/MO, SVC, TP Hub, HO)	Requisite bandwidth details have been provided in the RFP
63	94	Technical Specifications EMS	#102/Security & Patch Management	Proposed solution should have the ability to throttle bandwidth, either statically or dynamically. The throttling capability must support up and down stream throttling for both the server and agents	Can the patch management solution provide bandwidth throttling functionality for Desktop and servers only for downstream throttling as upstream throttling does not push too much data to the servers hence it is not required , Please clarify ?	Yes, the patch management solution should provide bandwidth throttling functionality for Desktop and servers only for downstream throttling as upstream throttling does not push too much data to the servers. This would lead to additional query to the process.
64	94	Technical Specifications EMS	#108/Security & Patch Management	Proposed solution should have native support for high level of encrypted communications without any dependency on additional software, hardware, third party certificates or Certificate Authority	Will self signed certificate for SSL communication meet the requirement?	Yes
65	94	Technical Specifications EMS	#109/Security & Patch Management	Proposed solution should have the ability to do centralized patch management for PCs, Laptops, Servers	Please specify the OS flavors with version which needs to be addressed using patch management?	Windows and RHEL
66	95	Technical Specifications EMS	#117/Security & Patch Management	Proposed solution should support event-driven remediation.	Please provide detailed use case(s) for event driven remediation	Requisite details will be shared with the successful bidder
67	95	Technical Specifications EMS	#126/Security & Patch Management	Proposed solution should support regulatory specific reports	Please clarify the regulatory standard Oriental insurance is looking for reporting	The solution should support regulatory standard like NVD, NIST, SCAP.
68	95	Technical Specifications EMS	#127/Security & Patch Management	Proposed solution should be able to manually group computers together for deployment of patches. Proposed solution should provide the ability to dynamically group computers based on asset and software information	Please clarify if the manual grouping based on asset and software information meets the requirement ? Would replicating AD groups to the patch management system meets the requirement?	The solution should support manual grouping or replicating the AD structure and groups for policy deployment.
69	95	Technical Specifications EMS	#128/Security & Patch Management	Proposed solution should support the grouping of patches into a 'baseline' which can take the form of monthly patch bundle e.g. ' Critical Patches'	If the product provides the feasibility to manually create patch groups policy for deployment based on criticality would meet the requirement ?	The solution should manually create patch groups policy for deployment based on criticality.

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
70	96	Technical Specifications EMS	#132/Security & Patch Management	Proposed solution should be able to identify the computers that have installed the patch that is to be rolled back on need basis	If the solution provides report filter on patch(s) deployed to be rolled back would meet the requirement?	Please be guided by the RFP
71	96	Technical Specifications EMS	#133/Security & Patch Management	Proposed solution should be able to provide real-time (within minutes) patch deployment status monitoring	If the proposed solution be able to provide near real-time (within minutes) patch deployment status monitoring while agent communication and other network dependencies are taken care, meets the requirement?	Please be guided by the RFP
72	96	Technical Specifications EMS	#139/Security & Patch Management	Proposed solution should have the dashboard to drill down to show details for both compliant and non-compliant systems, including but not limited to, non-compliant controls, component name, category, identifier and type	If the proposed patch management solution provides compliant and non-compliant systems based on patch baseline meets the requirement ? Please clarify the details of noncompliant controls, component name, category, identifier and type	The solution should provide compliant and non-compliant systems based on patch baseline. The solution should display the applicable bulletins, applicable devices, compliant , non compliant, reboot pending as a part of reporting.
73	96	Technical Specifications EMS	#140/Security & Patch Management	In the proposed solution, information reported should not be more than 1-7 days old for devices that are active on the network	Please clarify if the devices are not connected to the network for more than 7 days, then this should be reported for patch compliance or not?	Yes
74	97	Technical Specifications EMS	#145/Security & Patch Management	Proposed solution should allow console operator to trigger alerts when user-defined conditions are met	If the proposed EDR solution meets the requirement and this requirement can be eliminated from patch management requirement?	Please be guided by the RFP
75	97	Technical Specifications EMS	#148/Security & Patch Management	Proposed solution should have automatic patch management and deploy patches for various platforms including Windows, Linux/Unix, Solaris and AIX	Please specify if Windows and Linux OS support for patch management suffice the requirement ?	Yes
76	97	Technical Specifications EMS	#150/Security & Patch Management	In the proposed solution, reports should be viewed online	Please clarify if online depicts the web interface ?	Please be guided by the RFP

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
77	97	Technical Specifications EMS	#151/Security & Patch Management	In the proposed solution, reports should be downloaded in CSV, PDF, TXT and XML formats	Please clarify, if the proposed solution provides the functionality to save report in CSV , XLS & HTML will meet the requirement?	Bidder to note that the solution should provide the functionality to **save** report in CSV, XLS format
78	20	Scope of Work	2.3.1 Sizing of Hardware	The proposed solution should be in HA at DC & DR.	Please confirm if OICL is looking for HA in DC and HA in DR both or HA in DC and DR as standalone (DC will act as Active-Passive and DC and DR will act as Active-Redundant)?	Bidder should consider HA (Active-Passive) between DC & DR. HA (Active-Active) at DC and HA (Active-Passive) at DR
79	86	Technical Specifications EMS	EMS	5. The solution should be capable of managing business service events by exploiting agent/agentless data sources and be able to do automatic provisioning of management policies and monitoring templates which are parameterized to specific CI instances in an automatically discovered run time service model with an additional provision to integrate with 3rd party CMDBs and also provide a self-service portal for administrators	Which of the monitoring parameters are requried to be monitored using agentess monitoring?	We have given the options for agent or agentless monitoring. OEM can choose either solution/approach which meets the technical specifications of EMS as provided in the RFP. Monitoring parameters should as per product support as defined in the RFP.
80	87	Technical Specifications EMS	EMS	20. It should provide Software Compliance, Contract Management and Financial Charge back capabilities that go beyond asset tracking and provide complete Asset lifecycle management; that provide a real Return On Investment for IT organizations	Please provide the list of softwares for which software compliance is needed?	Software compliance should be as per- supported by product out of the box.
81	88	Technical Specifications EMS	EMS	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 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	This point is more related to application performance monitoring which is not the standard requirement of RFP. Requesting OICL customer to remove this point from the compliance point.	Clause stands deleted

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
82	88	Technical Specifications EMS	EMS	31. Support for backup and storage	Requesting OICL to provide the clarity on this compliance requirement? If it is related to system and application backup then it must be done by the backup software, please confirm if it is the correct understanding?	Yes it is related to system and application backup. Bidder to ensure that they use backup software to take back up for application and system back up as provided by OICL.
83	88	Technical Specifications EMS	EMS	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.	Requesting customer to remove the single family/suite clause as this is favouring to specific OEM and stopping enterprise OEM's to participate on this RFP.	Revised clause reads: The modules/products should be from COTS OEM so as to ensure the integration and high level of data exchange between various layers.
84	89	Technical Specifications EMS	EMS	44. Capability of integrating with third party element manager	Please mention the third party element manager names and versions to check the integration feasibility with EMS solution along with number of instances.	Only solution capability is required
85	89	Technical Specifications EMS	EMS	44. Capability of integrating with third party element manager	Please confirm if third party element manager does support REST API or SNMP Trap forwarding integration capabilities for integration with proposed EMS solution?	Only solution capability is required
86	90	Technical Specifications EMS	EMS	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	Monitoring the HTTP is the part and standard offering of Application Performance Monitoring tool. Requesting OICL to remove this keyword from the compliance point.	Clause stands deleted
87	90	Technical Specifications EMS	EMS	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	Dedicated Data Collector is needed in any specific location or all devices can be directly reachble to Data Center ?	Clause stands deleted
88	91	Technical Specifications EMS	EMS	68. The proposed solution should provide built-in reporting functionality	Please share few sample reports which you are expecting to validate the need of external reporting solution?	Requisite details will be shared with the successful bidder

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
89	93	Technical Specifications EMS	EMS	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.	Cumulative return on investment (ROI) and most frequent resolution workflow are not the standard feature of helpdesk and automation tool. Requesting customer to remove these keywords from the compliance point.	Clause stands deleted
90	100	Technical Specifications EMS	Helpdesk Solution	7.4 Upon submission, every request should be assigned with unique-id which shall remain unique through-out 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)	Customize the number ex.date-month-branch ID - type of asset-xx is not possible. Requesting customer to remove this statement from this compliance point.	Clause stands deleted
91	100	Technical Specifications EMS	Helpdesk Solution	8. Engineer Availability / Attendance tracking	Attendance tracking is not the standard offering of Helpdesk solution. MSI/Customer can use HR or attendance tracking system for this purpose. Hence requesting OICL to remove this section from the compliance point.	Clause stands deleted
92	104	Technical Specifications EMS	Helpdesk Solution	30. Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.	What is expected in multi-tenancy configuration. Is this required in the proposed solution. If yes, for what are the modules it is neededd ?	Only solution capability is required

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
93	106	Technical Specifications EMS	Asset Discovery Specifications	3. Discovery system should have the ability to capture configuration files for the purposes of comparison and change tracking.	Discovery solution do not capture the log file for comparison and change tracking and it is also not the standard feature of discovery solution. Hence Requesting customer to modify this compliance point as follows: "Discovery system should have the ability to capture configuration changes for the purposes of comparison and change tracking."	Revised clause reads: Discovery system should have the ability to capture configuration changes for the purposes of comparison and change tracking.
94	107	Technical Specifications EMS	Discovery	8. Discovery system should have ability to modify out-of-box discovery scripts, create customized discovery scripts.	what type of devices requirs the customized discovery ?	Requisite details will be shared with the successful bidder
95	107	Technical Specifications EMS	Discovery	11. Proposed Tool should support discovery of VMware storage topology including VMware data stores, VM file systems, local storage on the ESX servers and the relations between them.	Please provide the ESXi version details?	Requisite details will be shared with the successful bidder
96	107	Technical Specifications EMS	Discovery	12. Proposed Tool must support storage elements discovery, including storage arrays, logical disks, and interconnectivity between SAN elements.	Storage models, vendor details are required for validation?	Requisite details will be shared with the successful bidder
97	107	Technical Specifications EMS	Discovery	13. Proposed Tool must support, system Center Virtual Machine Manager (SCVMM) Discovery and VMware vRealize Operations Manager (vROps) and Red Hat Virtualization Discovery to get infra/hosts details from virtualization platform.	Need the SCVMM and Vrops Version details	Requisite details will be shared with the successful bidder

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
98	30	Scope of Work	2.3.13 Escrow	OICL and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to OICL for EMS & Helpdesk Solution in order to protect its interests in an eventual situation. OICL and the selected bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Vendor	Requesting OICL authority to remove this clause and section from the RFP, as it will impossible for OEM to provide the source code because it is their Proprietary and cannot be shared with anyone	Please be guided by the RFP. Escrow is only for deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to OICL for EMS & Helpdesk Solution.
99	85	General	EMS	General Query for EMS Volumetric perspective	The proposed IT Service Management OEM must be an industry standard, enterprise grade solution and shall be present in either Leaders or Challengers (Strong Performers / Major Players) Quadrant of Forrester / Gartner / IDC report for ITSM in the last 3 published reports.	Please be guided by the RFP

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
100	85	General	EMS	Additional Point	Requesting customer to provide the following volumetric for Infrastructure volumetric count? Please confirm the infrastructure volumetric count: 1. No. of network devices to be monitored (SNMP/ICMP)? 2. Total no. of Physical servers? 3. Total no of Virtual Servers? 4. Total no. of Storage devices along with storage models and vendors? 5. Total nos. of DB OS instances to be monitored? 6. No. of Application OS Instance means an OS instance (physical or virtual machine) that runs an application component to be monitored? 7. Total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system? 8.Helpdesk Analyst Type - Concurrent or Named? 9. Total no. of Client OS instances(desktops/laptops) for asset management & tracking? 10. Any specific Integrations with EMS/NMS solution? 11. Total node counts for Integration with EMS solution? **Reason:** This will provide all the qualified EMS OEM's to participate equally technically and commercially.	1. No Network devices are being monitored 2. Monitoring is required only for the Hardware (physical/virtual) used to run the applications under this project i.e. AD,AV, EDR and EMS etc. 3. Monitoring is required only for the Hardware (physical/virtual) used to run the applications under this project i.e. AD,AV, EDR and EMS etc. 4. Storage is not required and will be provided by OICL. 5. Not Required 6. Not Required 7. There are a total of 34 helpdesk agents that are logging in the system. Bidder as part of this RFP is reqd. to propose the licenses as per count 8. Bidder to propose to ensure it meets the requirements of teh RFP 9. 10,000 10. List of solutions with which EMS needs to be integrated will be defined during SRS Phase. 11. 10,000

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
101	85	General	EMS	Additional Point	To ensure the mature security standard of proposed solution, SI must ensure that the proposed ITSM, ITAM and Asset Discovery solution OEM is ISO 27034 certified from one of the following certification agencies: Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte. Documentary proof must be provided at the time of submission.	Please be guided by the RFP
102	85	General	EMS	Additional Point	OEM should have min turnover of INR 70 Crores and above in each year in last 3 years. Audited Balance sheet should be provided.	Not Accepted. Please be guided by the RFP
103	17	Project Timeline	1.7 Project Timeline	1. Activity Directory Upgrade T+1.5 Month 2. Anti - Virus with EDR T+2 Month 3 Enterprise management System T+3 Month 4. Helpdesk Solution T+3 Month	**1. Activity Directory Upgrade T+3 Month** **2. Anti - Virus with EDR T+5 Month** **3 Enterprise management System T+5 Month** **4. Helpdesk Solution T+6 Month**	Please refer Corrigendum for revised timelines for Anti-Virus with EDR No change in timeline for Active Directory, EMS & Helpdesk Solution
104	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 1.1	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Please refer Corrigendum for revised specifications
105	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications- 2.5	The proposed solution should provide performance control while scanning files/folders/Hard disk	The proposed solution should provide performance control/optimized scan while scanning files/folders/Hard disk **justification**- Change in language to have clarity on the use case.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
106	80	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications-2.8	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser and should support majority of browsers Chrome, Edge, Safari, Firefox, Brave **justification**- Solution should offer the comprehensive coverage for most complete security.	Please refer Corrigendum for revised specifications
107	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -8	Additional point: EDR	The solution must block the OICL user from using it's corporate credentials in a untrusted site that does not belong to corporate credential domain to secure the user identity and the credentials. Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's & leverage application of AI & ML to meet this requirement. **justification** - Use of stolen credentials is most used tactics by cyber criminals to get the initial access by Ransomware actors. As per Verizon data breach report Credentials & Phishing are top two path leading to your state a.k.a entry point for the Cyber criminals. ref- https://www.verizon.com/business/resources/reports/dbir/	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
108	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.1	2.3.3 Antivirus Solution with EDR Functionality	We understand that End Point Protection security controls NGAV, EDR (Anti-Exploit, Anti Ransomware Protection) & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications
109	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications	The proposed solution should be purpose build, unified agent for all features with on-premise architecture	We understand that End Point Protection security controls NGAV, EDR & Encryption may require multiple licenses/agents. Hence we request OICL to separately share specifications for these so that any overlap security capabilities can be avoided.. Also provide the clarification on the maximum number of agents to be factored to meet the technical requirement.	Please refer Corrigendum for revised specifications
110	22	Scope of Work AV + EDR	2	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with Windows operating system for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with **Open Servers & Windows server/endpoint** for management, intermediatory & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.	Please be guided by the RFP

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
111	79	Technical Specifications; AV + EDR	10.1 Appendix 1: Technical Specifications -1.11	The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response	Our understanding is that end point anti-apt sandboxing solution has to be natively integrated into EDR capabilities and all the required hardware to be factored for on-premise deployment. We request you to provide clarification in this regards and change the requirements The proposed solution should have the following protection mechanism: Anti-Malware, anti-ransomware protection Host Intrusion Prevention System / Anti exploit module Application Control & Disk encryption Zero Phishing & end point compliance Endpoint Detection & Response, Anti-APT	Please refer Corrigendum for revised specifications
112	94	Technical Specifications EMS	Annexure 10, 110	Proposed solution should support the IPv4 & IPv6	Most of the solutions are IPv4 compliant today and IPV6 will be in road map, can we make it IPV4 only .	Please be guided by the RFP
113	99	Technical Specifications EMS	Annexure 10, 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.	Request you to kindly make it Pink verify 2011 with minimum 3 process. As very few OEMS will be have Pink verify- 4 and more than 3 proesses	Revised clause reads: 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,

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
						Knowledge Management, IT Asset Management and Service Request Management.
114	105	Technical Specifications EMS	Annexure 10, 27.2	Dynamic configuration changes shall be possible without having to reboot the box.	Dynamic configuration of the ITSM tool you mean here ? Pls provide clarity.	Yes, changes related to tool
115		Technical Specifications EMS		Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model.	IS this applicable for endpoints also or only limited to network devices ?	Please be guided by the RFP
116		General	General		Count of Technician license required for ITSM is not mentioned any where can we get that	OICL currently has 34 licenses. Bidder is required to propose licenses as per RFP Requirement.
117	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	We support windows operating systems which are under active windows support from Microsoft. As this contract is for 6 years and some of these OS will be going EOL from MS during that period the same will need to be upgraded to latest Win OS versions to keep continuing the AV support. We hope this is inline with OICL expectations.	Please refer Corrigendum for revised specifications
118	77	Technical Specifications; AV + EDR	1.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.	Our solution support Windows and Mac OS. For RHEL and Cent OS which are server OS we request you to kindly remove the same as the technical specifications for server OS will differ from desktop/windows environment. The server solution will have a different product and functionalities suited to server environment. We request you to define server technical requirements separately.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
119	77	Technical Specifications; AV + EDR	1.11.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Application Control & Disk encryption	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
120	77	Technical Specifications; AV + EDR	1.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Zero Phishing & end point compliance	We understand OICL is looking for anti phishng capability. If so kindly modify to 'anti phishing'	Please refer Corrigendum for revised specifications
121	77	Technical Specifications; AV + EDR	1.11.3.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Web based installation	We wish to highlight that this feature is not supported if OICL is using Server Core installation for Windows, kindly clarify if server core is being used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications
122	77	Technical Specifications; AV + EDR	1.11.3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Remote installation	Remote installation is not possible for Windows 8.1 (basic versions) and Windows 10 (Home Edition) kindly clarify if these OS versions are/will be used in OICL, if yes request you to delete this.	Please refer Corrigendum for revised specifications
123	79	Technical Specifications; AV + EDR	2.10/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as non-compliant and can apply restrictive policies to them.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
124	79	Technical Specifications; AV + EDR	2.11.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	windows services created by malware	Kindly modify to 'Kills processes that Trojans create'.	Please refer Corrigendum for revised specifications
125	79	Technical Specifications; AV + EDR	2.11.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	any other system settings affected by malware	Kindly modify 'Repairs system files that Trojans modify'.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
126	79	Technical Specifications; AV + EDR	2.17/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The proposed solution must provide application of enforcement actions based on malicious file types such as Delete, Block, Quarantine	Kindly delete 'Block' as malicious file will either be deleted or quarantined.	Please refer Corrigendum for revised specifications
127	79	Technical Specifications; AV + EDR	2.18/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Preventive controls from advanced sophisticated attack against users including Anti Phishing, Web form protection, account takeover protection etc.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
128	79	Technical Specifications; AV + EDR	2.19/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's :	Kindly modify 'Solution should be able to categorise phishing url using reputation engine.'	Please refer Corrigendum for revised specifications
129	79	Technical Specifications; AV + EDR	2.20/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Full disk encryption - All volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
130	80	Technical Specifications; AV + EDR	3.4/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution will protect against existing and zeroday ransomware without requiring signature updates. The anti-ransomware capability should have auto rollback feature to restore the system back to original state. The anti-ransomware solution has third party-validation.	Kindly delete 'third party validation'.	Please refer Corrigendum for revised specifications

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
131	80	Technical Specifications; AV + EDR	3.5/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution should support zero trust policy for files downloaded from untrusted sources on web. Solution must sanitize all the active content / scripts from the file before it deliver to end user.	Kindly delete this clause as it is more of web security feature.	Please refer Corrigendum for revised specifications
132	80	Technical Specifications; AV + EDR	4.2/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should allow for selection of Native encryption or BitLocker Management via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
133	80	Technical Specifications; AV + EDR	4.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	The solution should support seamless switching between BitLocker Management and Native encryption via policy.	We wish to highlight that the OICL requirement is combination of AV, EDR and Encryption which may require multiple agents/products, we request OICL to clearly bifurcate and define specifications for AV, EDR and Encryption to avoid any overlap.	Please refer Corrigendum for revised specifications
134	82	Technical Specifications; AV + EDR	7.3/ Appendix 1: Technical Specifications, Anti-Virus with EDR	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. (Data collected through post-event scripts or live interaction with host is covered in a separate requirement.) 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	Kindly delete '(Data collected through post-event scripts or live interaction with host is covered in a separate requirement.)'	Please refer Corrigendum for revised specifications
135	20	Scope of Work	2.3.1 Sizing of Hardware	The proposed solution should be in HA at DC & DR.	Please confirm if OICL is looking for HA in DC and HA in DR both or HA in DC and DR as standalone (DC will act as Active-Passive and DC and DR will act as Active-Redundant)?	Bidder should consider HA (Active-Passive) between DC & DR. HA (Active-Active) at DC and HA (Active-Passive) at DR

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
136	86	Technical Specifications EMS	EMS	5. The solution should be capable of managing business service events by exploiting agent/agentless data sources and be able to do automatic provisioning of management policies and monitoring templates which are parameterized to specific CI instances in an automatically discovered run time service model with an additional provision to integrate with 3rd party CMDBs and also provide a self-service portal for administrators	Which of the monitoring parameters are required to be monitored using agentless monitoring?	We have given the options for agent or agentless monitoring. MSI/OEM can go with any of solution/approach which must meet the technical specifications of EMS as provided in the RFP. Monitoring parameters should as per product support as defined in the RFP.
137	87	Technical Specifications EMS	EMS	20. It should provide Software Compliance, Contract Management and Financial Charge back capabilities that go beyond asset tracking and provide complete Asset lifecycle management; that provide a real Return On Investment for IT organizations	Please provide the list of software for which software compliance is needed?	Software compliance should be as per supported by product out of the box.
138	88	Technical Specifications EMS	EMS	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 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	This point is more related to application performance monitoring which is not the standard requirement of RFP. Requesting OICL customer to remove this point from the compliance point.	Requisite details will be shared with the successful bidder
139	88	Technical Specifications EMS	EMS	31. Support for backup and storage	Requesting OICL to provide the clarity on this compliance requirement? If it is related to system and application backup then it must be done by the backup software, please confirm if it is the correct understanding?	Requisite details will be shared with the successful bidder

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
140	88	Technical Specifications EMS	EMS	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.	Requesting customer to remove the single family/suite clause as this is favouring to specific OEM and stopping enterprise OEM's to participate on this RFP.	Revised clause reads: The modules/products should be from COTS OEM so as to ensure the integration and high level of data exchange between various layers.
141	89	Technical Specifications EMS	EMS	44. Capability of integrating with third party element manager	Please mention the third party element manager names and versions to check the integration feasibility with EMS solution along with number of instances.	Only solution capability is required
142	89	Technical Specifications EMS	EMS	44. Capability of integrating with third party element manager	Please confirm if third party element manager does support REST API or SNMP Trap forwarding integration capabilities for integration with proposed EMS solution?	Only solution capability is required
143	90	Technical Specifications EMS	EMS	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	Monitoring the HTTP is the part and standard offering of Application Performance Monitoring tool. Requesting OICL to remove this keyword from the compliance point.	Monitoring the HTTP is the part and standard offering of Application Performance Monitoring tool. Requesting OICL to remove this keyword from the compliance point.
144	90	Technical Specifications EMS	EMS	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	Dedicated Data Collector is needed in any specific location or all devices can be directly reachable to Data Center ?	Clause stands deleted
145	91	Technical Specifications EMS	EMS	68. The proposed solution should provide built-in reporting functionality	Please share few sample reports which you are expecting to validate the need of external reporting solution?	Requisite details will be shared with the successful bidder

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
146	93	Technical Specifications EMS	EMS	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.	Cumulative return on investment (ROI) and most frequent resolution workflow are not the standard feature of helpdesk and automation tool. Requesting customer to remove these keywords from the compliance point.	Clause stands deleted
147	100	Technical Specifications EMS	Helpdesk Solution	7.4 Upon submission, every request should be assigned with unique-id which shall remain unique through-out 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)	Customize the number ex.date-month-branch ID - type of asset-xx is not possible. Requesting customer to remove this statement from this compliance point.	Clause stands deleted
148	100	Technical Specifications EMS	Helpdesk Solution	8. Engineer Availability / Attendance tracking	Attendance tracking is not the standard offering of Helpdesk solution. MSI/Customer can use HR or attendance tracking system for this purpose. Hence requesting OICL to remove this section from the compliance point.	Clause stands deleted
149	104	Technical Specifications EMS	Helpdesk Solution	30. Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.	What is expected in multi-tenancy configuration? Is this required in the proposed solution? If yes, for what are the modules it is needed?	Only solution capability is required

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
150	106	Technical Specifications EMS	Asset Discovery Specifications	3. Discovery system should have the ability to capture configuration files for the purposes of comparison and change tracking.	Discovery solution do not capture the log file for comparison and change tracking and it is also not the standard feature of discovery solution. Hence Requesting customer to modify this compliance point as follows: "Discovery system should have the ability to capture configuration changes for the purposes of comparison and change tracking."	Revised clause reads: Discovery system should have the ability to capture configuration changes for the purposes of comparison and change tracking.
151	107	Technical Specifications EMS	Discovery	8. Discovery system should have ability to modify out-of-box discovery scripts, create customized discovery scripts.	what type of devices requires the customized discovery ?	Requisite details will be shared with the successful bidder
152	107	Technical Specifications EMS	Discovery	11. Proposed Tool should support discovery of VMware storage topology including VMware data stores, VM file systems, local storage on the ESX servers and the relations between them.	Please provide the ESXi version details?	Requisite details will be shared with the successful bidder
153	107	Technical Specifications EMS	Discovery	12. Proposed Tool must support storage elements discovery, including storage arrays, logical disks, and interconnectivity between SAN elements.	Storage models, vendor details are required for validation?	Requisite details will be shared with the successful bidder
154	107	Technical Specifications EMS	Discovery	13. Proposed Tool must support, system Center Virtual Machine Manager (SCVMM) Discovery and VMware vRealize Operations Manager (vROps) and Red Hat Virtualization Discovery to get infra/hosts details from virtualization platform.	Need the SCVMM and Vrops Version details	Requisite details will be shared with the successful bidder

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
155	30	Scope of Work	2.3.13 Escrow	OICL and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to OICL for EMS & Helpdesk Solution in order to protect its interests in an eventual situation. OICL and the selected bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Vendor	Requesting OICL authority to remove this clause and section from the RFP, as it will impossible for OEM to provide the source code because it is their Proprietary and cannot be shared with anyone	Please be guided by the RFP. Escrow is only for deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to OICL for EMS & Helpdesk Solution.
156	85	General	EMS	General Query for EMS Volumetric perspective	The proposed IT Service Management OEM must be an industry standard, enterprise grade solution and shall be present in either Leaders or Challengers (Strong Performers / Major Players) Quadrant of Forrester / Gartner / IDC report for ITSM in the last 3 published reports.	Please be guided by the RFP

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
157	85	General	EMS	Additional Point	Requesting customer to provide the following volumetric for Infrastructure volumetric count? Please confirm the infrastructure volumetric count: 1. No. of network devices to be monitored (SNMP/ICMP)? 2. Total no. of Physical servers? 3. Total no of Virtual Servers? 4. Total no. of Storage devices along with storage models and vendors? 5. Total nos. of DB OS instances to be monitored? 6. No. of Application OS Instance means an OS instance (physical or virtual machine) that runs an application component to be monitored? 7. Total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system? 8.Helpdesk Analyst Type - Concurrent or Named? 9. Total no. of Client OS instances(desktops/laptops) for asset management & tracking? 10. Any specific Integrations with EMS/NMS solution? 11. Total node counts for Integration with EMS solution? **Reason:** This will provide all the qualified EMS OEM's to participate equally technically and commercially.	1. No Network devices are being monitored 2. Monitoring is required only for the Hardware (physical/virtual) used to run the applications under this project i.e. AD,AV, EDR and EMS etc. 3. Monitoring is required only for the Hardware (physical/virtual) used to run the applications under this project i.e. AD,AV, EDR and EMS etc. 4. Storage is not required and will be provided by OICL. 5. Not Required 6. Not Required 7. There are a total of 34 helpdesk agents that are logging in the system. Bidder as part of this RFP is reqd. to propose the licenses as per count 8. Bidder to propose to ensure it meets the requirements of teh RFP 9. 10,000 10. List of solutions with which EMS needs to be integrated will be defined during SRS Phase. 11. 10,000

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
158	85	General	EMS	Additional Point	To ensure the mature security standard of proposed solution, SI must ensure that the proposed ITSM, ITAM and Asset Discovery solution OEM is ISO 27034 certified from one of the following certification agencies: Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte. Documentary proof must be provided at the time of submission.	Please be guided by the RFP
159	85	General	EMS	Additional Point	OEM should have min turnover of INR 70 Crores and above in each year in last 3 years. Audited Balance sheet should be provided.	Please be guided by the RFP
160	16	Eligibility Criteria	1.6 Eligibility Criteria	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in the last five (5) years. A. Proposed EMS Solution in a BFSI/ PSU/ Government Organization in India with at least 7,500 employees B. Endpoint Security with at least 7,500 endpoints in a BFSI/ PSU/ Government Organization in India	It is requested that clause may be amended as: Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in the last five (5) years. A. EMS Solution in a BFSI/ PSU/ Government Organization in India with at least 7,500 employees B. Endpoint Security with at least 1,000 endpoints in a BFSI/ PSU/ Government Organization in India	Please be guided by the RFP
161	47	Eligibility Criteria	Section 6.4: Eligibility cum Technical Evaluation	Proposed EMS Solution with at least 7,500 employees	Please amend the clause as "Proposed EMS/ NMS solution with at least 7,500 employees" It is requested that EMS/ NMS option may please be given as NMS is a broader term and can control many EMS and also control them. EMS usually manages single element or group of similar element whereas NMS manages complete network.	Please be guided by the RFP
162	47	Eligibility Criteria	Section 6.4: Eligibility cum	Endpoint Security with at least 7,500 endpoints	Please amend the clause as "Endpoint Security with at least 200 endpoints" in order to increase the competition.	Please be guided by the RFP

Reply to Pre- Bid Queries

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

#	Page #	Section	Point/ Section #	Existing Clause	Query Sought	OICL's Response
			Technical Evaluation			
163	16	Eligibility Criteria	Clause : 1.6 Eligibility Criteria Clause No. 10	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in last five (5) years. 1. Proposed EMS solution in a BFSI/PSU/Government Organization in India with at least 7,500 employees 2. Endpoint Security with at least 7,500 endpoints in a BFSI/PSU/ Government Organization in India 3. AD Upgrade/ Implementation in a BFSI/ PSU/ Government Organization in India	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in last five (5) years. 1. ~~Proposed~~ EMS solution in a BFSI/PSU/Government Organization in India with at least 7,500 employees 2. Endpoint Security with at least 7,500 endpoints in a BFSI/PSU/ Government Organization in India 3. AD Upgrade/ Implementation in a BFSI/PSU/Government Organization in India	Please be guided by the RFP
164	47	Technical Evaluation Criteria	Clause : 6.4 Eligibility cum Technical Evaluation Clause No. 4	Bidder's Past Experience of having supplied, implemented and maintained/maintaining: Max. Marks- 100 marks Proposed EMS solution with at least 7,500 employees	Bidder's Past Experience of having supplied, implemented and maintained/maintaining: Max. Marks- 100 marks ~~Proposed~~ EMS solution with at least 7,500 employees	Please be guided by the RFP
165	47	Technical Evaluation Criteria	Clause : 6.4 Eligibility cum Technical Evaluation Clause No. 4	Bidder's Past Experience of having supplied, implemented and maintained/maintaining: Max. Marks- 100 marks Endpoint Security with at least 7,500 endpoints In at least one BFSI/ PSU/ Government Organization in India- 35 marks More than one BFSI/PSU/Government Organization in India- 50 marks	Bidder's Past Experience of having supplied, implemented and maintained/maintaining: Max. Marks- 100 marks Endpoint Security with at least 7,500 endpoints In at least one BFSI/ PSU/ Government Organization in India- 40 marks More than one BFSI/PSU/Government Organization in India- 45 marks	Please be guided by the RFP