

Corrigendum to the Tender 300000331 dated 04.09.2017

As per Tender document pre bid meeting was held on 19.09.2017 in Mazagon Dock Shipbuilders Limited. The changes in technical specification, scope of work is mentioned below according to query raised by bidders in Pre bid meeting. All other tender terms & conditions including tender closing date remains unchanged.

Sr.No	Page	Clause	Existing Clause Details	To be read as
1	17	2.4	2.4 E-mail solution from Lotus notes 9 or any webmail system which may come in future	2.4 Netcore emergic mailing solution with 2000 user licenses.
2	17	4.4	4.4 Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	4.4 Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp.
3	18	4.19	4.19 The Bidder has to audit the DLP solution setup in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor.	4.19 The Bidder has to get the DLP solution setup audited in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor. Also the OEM has to certify the ready to use of the DLP solution.
4	19	5.5.5	5.5.5 Capability to Monitor all traffic flowing out of the Network, irrespective of Policies being in place or not.	5.5.5 Deleted
5	20	5.6.18	5.6.18 DLP Solution should provide broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the flexible response feature, such as applying encryption to a file using	5.6.18 Deleted
6	21	6.1.1.	6.1.1 2 CPU Server - 2 nos, each CPU with 14 cores with VMware 6.5 enterprise installed and O/s Windows Server 2012. Any different O/s requirement of the proposed product, the same has to be provided the bidder.	6.1.1 For Primary - 2 CPU Server - 2 nos, each CPU with 14 cores with VMware 6.5 enterprise installed and O/s Windows Server 2012 and for Near DR - 2 CPU Server - 2 nos, each CPU with 14 cores with VMware 6.5 enterprise installed and O/s Windows Server 2012. Any different O/s requirement for the proposed product, the same has to be provided the bidder.
7	21	6.1.2	6.1.2 Storage SAN Fujitsu DX 5300 with sufficient Disk capacity and storage replication enabled.	6.1.2 2 Sets of Storage (Primary & Near DR each) SAN Fujitsu DX 5300 with sufficient Disk capacity and storage replication enabled.

Sr.No	Page	Clause	Existing Clause Details	To be read as
8	21	6.3	6.3 The Hardware (Server) of HP / Dell / Fujitsu / Cisco / Hitachi make & software (DLP, O/S, Databases and any other software) for the DLP setup for the Internet machines supply & installation is bidder's scope. Rack mounted server should be provided. Intel xeon with minimum dual CPU with 8 cores per CPU, 256GB RAM and 5TB SSD Hard disk in the rack mounted server with mounting rail kit. Bidder to do Fitment of Rack server in existing rack. In case of hard disk failure, the faulty hard disk cannot be taken out of MDL premises. Vendor has to provide a replacement for the faulty hard disk at no extra cost. The vendor shall bring their licensed data recovery software and all efforts to recover the data from the failed hard disk have to be carried out.	6.3 The Hardware (Server) of HP / Dell / Fujitsu / Cisco / Hitachi make & software (DLP, O/S, Databases and any other software) for the DLP setup for the Internet machines supply & installation is bidder's scope. Rack mounted server should be provided. Intel xeon with minimum dual CPU with 8 cores per CPU, 256GB RAM and 5TB SSD Hard disk in the rack mounted server with mounting rail kit. Bidder to do Fitment of Rack server in existing rack. In case of hard disk failure, the faulty hard disk cannot be taken out of MDL premises. Vendor has to provide a replacement for the faulty hard disk at no extra cost. The vendor shall bring their data recovery software and all efforts to recover the data from the failed hard disk have to be carried out.
9	22	7-100	7.100 Data Loss/Leakage prevention software for endpoint, network (100 server nodes to be installed on a virtual environment), encryption at file, folder & removable media & discovering of sensitive, confidential data for LAN setup (including software, operating system, Database licenses)for 2500 nos devices and 250 nos drive/disk encryption considering the primary, Near DR site and for Internet machines setup.	7.100 Data Loss/Leakage prevention Software for Endpoint, network, Email, encryption at file, folder & removable media & discovering of sensitive, confidential data for LAN setup (including software, operating system, Database licenses) considering 2500 nos devices, 100 server nodes on Linux, and 250 nos drive/disk encryption considering the primary, Near DR site and for Internet machines setup.
10	22	7-300	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, Arc Sight SIEM etc)
11	22	8.1.1	8.1.1 Step 1 Data Flow Analysis (DFA) -Bidder has to carry out detailed DFA by consultant, experienced in this area and CISA certified by coordinating with various people, stakeholders / departments, processes and prepare the Data Flow Analysis (DFA), information classification, business & technical requirement and the Policies to be implemented. Deliverable will be final sign off from stakeholders, DFA, information classification policies, best practices for storage of data across organization, DLP security Policies to be implemented.	8.1.1 Step 1 Data Flow Analysis (DFA) –OEM has to carry out detailed DFA (Confirmation from the OEM to be submitted with the technical bid) by coordinating with various people, stakeholders / departments, processes and prepare the Data Flow Analysis (DFA), information classification, business & technical requirement and the Policies to be implemented. Deliverable will be final sign off from stakeholders, DFA, information classification policies, best practices for storage of data across organization, DLP security Policies to be implemented.
12	23	9.5	9.5 Customization: Selected bidder shall customize the system as per the requirements of the MDL without any additional cost to the MDL. Customization of the solution would be treated as complete on successful User Acceptance Test. The MDL team shall be included in the process so that they are able to understand the details of the system and process.	9.5 Configuration: Selected bidder shall configure the system as per the requirements of the MDL without any additional cost to the MDL. Configuration of the solution would be treated as complete on successful User Acceptance Test. The MDL team shall be included in the process so that they are able to understand the details of the system and process.

Sr.No	Page	Clause	Existing Clause Details	To be read as
-------	------	--------	-------------------------	---------------

Sr.No	Page	Clause	Existing Clause Details	To be read as
-------	------	--------	-------------------------	---------------

Note:

1. Please find attached enclosure for more details.
2. In case of any clarifications, bidders are requested to contact to Commercial section Tel: 022-2376 2220/2240 well in advance of the closing date of the tender.
3. In case bidder encounters any technical snag pertaining to e-procurement system while acting on the tender, computer screen shot of the error message with date & time stamp on the web-browser along with the query shall be e-mailed by the bidder to the help desk (as mentioned 2.6 above) for problem resolution at least 72 hours before the due date and time of the tender.
4. Bidders should login well in advance to enable them to complete their bid submission before the closing time of the tender since the e-procurement system does not permit submission of any offer after closing date and time of the e-tender. Bidders are also requested to submit their bid well in advance to avoid last minute frantic calls.

संलग्नपत्र / Enclosures:

Enclosure-1: Clarifications on Vendor queries during Pre bid meet.

Sub: Reply to Prebid Queries - Tender 3000000331 dated 04.09.2017

The clarifications to the prebid queries and the changes with respect to the technical specifications is indicated below.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
5	17	2.2	Project Requirements does not cover near DR site and DR site.	PI confirm.	This is existing set up in MDL.
	17	2.4	E-mail solution from Lotus notes 9 or any webmail system which may come in future	Please mention the proposed email system and users base	Netcore emergic mailing solution with 2000 user licenses.
4	17	3.1	MDL has more than 2500 PCs, Laptops, workstations & servers.	need to know the Operating system across them all.	Windows client (Vista to 10.0), Windows Servers (2008, 2012, 2016) Red Hat Linux 6.0 and above, Suse Linux 11.0 and above
6	17	3.1	Disk Encryption is required for 250 nos machines.	Are they included in 2500 or are additional ?	Yes They are included in 2500
19	17	3.1	3. Project Requirements 3.1 DLP solution for securing for 2500 PCs, Laptops, workstations & servers with Endpoint, Network , Discovery and Encryption at File, Folder and removable media Level. Disk Encryption is required for 250 nos machines.	Can you please provide us the split per - PC - Laptops - Workstations -Servers Also you are mention 100 servers, are these servers part of the same 2500 endpoint or aditional.	The count including PC/Laptops/Workstations/windows servers is 2500 nos. The 100 servers (which are Linux based) are not part of this 2500.
	17	3.1	Disk Encryption is required for 250 nos machines.	Can we provide a separate Disk Encryption solution for the 250 users ?	Encryption OEM for all type of encryption (file folder and Disk) should be one.
5	5	3.2	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores. One completed order with implementation of setup of minimum 2500 DLP licenses. Order copies & work completion certificates to be appended	Do we need to give the PO's of the proposed technology or any other OEM will do.	Yes, Bidder has to give PO issues in their name of similar supplies. Even PO of OEM other than proposed OEM issued in the name of bidder will be acceptable.
4		3.2	List of equipment held by them with model / year / working status along with details of their manufacturing facilities and personnel with designation, qualification and experience to determine their capabilities. SSI/NSIC units can alternatively submit valid certificate indicating their capacity.	Please elaborate, we are not a manufacturing unit but a reseller of the solution	You need to submit the engineers details with the qualifications. For equipment, bidder may like to quote deviation.
	17	3.3	Implementation period – 16 weeks which includes Data Flow Analysis(DFA), supply of licenses, implementation of the setup and classifying, discovering the sensitive, confidential data with MDL and configuring the policies, implementation of reports and alerts in the system.	Request to change timeframe to 22 weeks as there are a number of public and festival holidays that are scheduled towards the end of the year. The DFA task for a firm of given size would also involve	No Change

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
5		4	End User License Agreement (EULA)/Service level Agreement (SLA): If SLA/EULA needs to be signed for this contract, bidder should submit complete SLA/EULA format including all terms and conditions along with technical bid. Placement of order will be done only after mutual agreement of terms and conditions in SLA/EULA by both the parties and will be signed after placement of order by both the parties. Note: Purchase Order will be the primary document in all respects and SLA/EULA will be part of Purchase Order.	This will be issued by OEM - Please clarify	Draft of all required documents to be given at the time of submission of bid.
7	17	4.1	formulation of policies, alerts for DLP	Are they in place or yet to be prepared ?	Bidder to prepare DFA & formulate the policies.
9	18	4.10	4.10 MDL is in process of evaluating DRM (Digital Right Management) solutions. Bidder should have standard connector or create connector for DRM solutions like Seclore or equivalent. Bidder should co-ordinate with the DRM solution vendor for implementation of connectivity between the DRM & DLP solution within the tenure of Contract period.	Bidder expects MDL to co-ordinate with their vendors to meet expectations of our Solution.	Bidder should co-ordinate with the DRM solution for implementation of connectivity between the DRM & DLP solution within the tenure of Contract period. MDL will be facilitator.
	18	4.10	MDL is in process of evaluating DRM (Digital Right Management) solutions. Bidder should have standard connector or create connector for DRM solutions like Seclore or equivalent. Bidder should co-ordinate with the DRM solution vendor for implementation of connectivity between the DRM & DLP solution within the tenure of Contract period.	Integration with 3rd Party solutions such as DRM are done using remediation script. In all cases the connector needs customization, configuration and deployment to suite the context of the client. None of the DLP vendors have an official price component either. Request that we change the statement to read as below for RFP qualification as Legal would object to the same. "MDL is in process of evaluating DRM (Digital Right Management) solutions. Bidder should have standard connector or create connector for DRM solutions or connect via remediation scripts like Seclore or equivalent. Bidder should co-ordinate with the DRM solution vendor for implementation of connectivity between the DRM & DLP solution within the tenure of Contract period."	No change
3		4.13	4.13 Separate DLP setup for the Internet Facing standalone machines to be deployed for data protection in MDL.	Need To know How many such machines ?	150

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
21	18	4.13	4.13 Separate DLP setup for the Internet Facing standalone machines to be deployed for data protection in MDL.	Can you please provide more informations on what are you requesting by separate DLP for Internet Facing ?Can you please provide us the number of machines required for such set-up?	150
1		4.14	4.14 Rack mounted server inclusive of OS, Database licenses for DLP solution for Internet facing standalone machines, to be provided by Bidder. Bidder to do Fitment of Rack server in existing rack.	Is this for DMZ only? What if the solution provided is a software based solution? Can MDL provide VM ?	Bidder has to quote for the server with for Internet facing machines. Refer clause 6.3
4		4.18	4.18 The proposed DLP solution should be in the Gartner Magic Quadrant for DLP consecutively for at least last 3 years i.e. 2015-2017.	Data Resolve has been recognised by Data Security Council of India (DSCI).	No change
6	18	4.19	The Bidder has to audit the DLP solution setup in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor.	Who will appoint the CERT-IN empanelled auditor vendor or MDL? Audit to be conducted against which standards	The bidder has to appoint a CERT-In empaneled auditor. (audit of VAPT, hardening of h/w, O/s, S/w needs to be done). And application point of view, OEM has to certify for ready to use.
12	18	4.19	The Bidder has to audit the DLP solution setup in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor.	Who are empanelled auditors? Is there any cost involved for conducting this audit or MDL will bear the cost.	The bidder has to appoint a CERT-In empaneled auditor. (audit of VAPT, hardening of h/w, O/s, S/w needs to be done). And application point of view, OEM has to certify for ready to use.
6	18	4.19	The Bidder has to audit the DLP solution setup in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor.	Who will appoint the CERT-IN empanelled auditor vendor or MDL? Audit to be conducted against which standards	The bidder has to appoint a CERT-In empaneled auditor. (audit of VAPT, hardening of h/w, O/s, S/w needs to be done). And application point of view, OEM has to certify for ready to use.
7	18	4.19	The Bidder has to audit the DLP solution setup in MDL by CERT-In empanelled auditor before put in to the production. The bidder has to carry out the changes in the setup to comply with the recommendations and get compliance certificate from the CERT-In empanelled auditor.	Who will appoint the CERT-IN empanelled auditor vendor or MDL? Audit to be conducted against which standards	The bidder has to appoint a CERT-In empaneled auditor. (audit of VAPT, hardening of h/w, O/s, S/w needs to be done). And application point of view, OEM has to certify for ready to use.
10	18	4.19	CERT-In empanelled auditor	Who are they ?	They Auditors Empanelled by CERT India. The List of auditors is there on the CERT India Website.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
11	18	4.21	MDL may visit the site of bidder's DLP customer place. Bidder should co-ordinate for visit	We can co-ordinate your visit. All arrangements and costing to be borne by MDL.	MDL desire bidder to co-ordinate the visit. MDL shall bear all the expenses for the visit of MDL personnel.
1		4.3	4.3 Sensitive / confidential data when sent by mail (web mail as well as client on Windows and Linux machines) should be monitored, encrypted & blocked.	How many machines are Linux OS ?	No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above
11	17	4.3	Sensitive / confidential data when sent by mail (web mail as well as client on Windows and Linux machines) should be monitored, encrypted & blocked.	Please clarify which email client based Windows and Linux is being used by Mazagon Dock. This point specific to single OEM and in order to promote fair competition, the mentioned statement should be amended to as follows: "Sensitive / confidential data when sent by mail should be monitored, encrypted & blocked."	We are accessing our mail using browser, the new mailing system will be from Netcore. No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above. No change.
1		4.3	Sensitive / confidential data when sent by mail (web mail as well as client on Windows and Linux machines) should be monitored, encrypted & blocked.	Please clarify which email client based Windows and Linux is being used by Mazagon Dock. This point specific to single OEM and in order to promote fair competition, the mentioned statement should be amended to as follows: " <i>Sensitive / confidential data when sent by mail should be monitored, encrypted & blocked.</i> "	We are accessing our mail using browser, the new mailing system will be netcore. No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above
	17	4.3	Sensitive / confidential data when sent by mail (web mail as well as client on Windows and Linux machines) should be monitored, encrypted & blocked	DLP solution will provide the monitoring and protection of the Web mail request over the gateway and also scan mail , and send to Encryption gateway rather than itself encrypting. Suggested change : Sensitive / confidential data when sent by mail (web mail as well as client on Windows and Linux machines) should be monitored, send to Encryption Gateway & blocked.	No change
4	17	4.4	Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	Is support for Linux system important? How many linux systems ? Are you also looking for a Mobile DLP solution or is it that the data should not be copied to mobile devices via USB? Data leakage through telnet is not possible suggest to remove telnet from the list	No desktop of Linux only servers are present. Currently 25 nos servers. Mobile DLP is not required. But data should not be leaked thru mobile connecting to computers.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
13	17	4.4	Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile , CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	Are you talking about MTP here	No desktop of Linux only servers are present. Currently 25 nos servers. Mobile DLP is not required. But data should not be leaked thru mobile connecting to computers.
2		4.4	4.4 Sensitive <i>j</i> confidential data should be monitored, encrypted and not able to be copied <i>j</i> sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet	How many machines are Linux OS ?	No desktop of Linux only servers are present. Currently 25 nos servers. Mobile DLP is not required. But data should not be leaked thru mobile connecting to computers.
4	17	4.4	Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	Is support for Linux system important? How many linux systems ? Are you also looking for a Mobile DLP solution or is it that the data should not be copied to mobile devices via USB? Data leakage through telnet is not possible suggest to remove telnet from the list	No desktop of Linux only servers are present. Currently 25 nos servers. Mobile DLP is not required. But data should not be leaked thru mobile connecting to computers. Telnet to be removed.
12	17	4.4	Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	Please clarify which email client based Windows and Linux is being used by Mazagon Dock. This point specific to single OEM and in order to promote fair competition, the mentioned statement should be amended to as follows: "Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	We are accessing our mail using browser, the new mailing system will be netcore. No desktop of Linux only servers are present. Currently 25 nos servers. Mobile DLP is not required. But data should not be leaked thru connecting mobile to computers. No Change.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
2		4.4	Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web as well as client on Windows and Linux machines), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet.	<p>Please clarify which email client based Windows and Linux is being used by Mazagon Dock.</p> <p>This point specific to single OEM and in order to promote fair competition, the mentioned statement should be amended to as follows:</p> <p><i>"Sensitive / confidential data should be monitored, encrypted and not able to be copied / sent through e-mail (web), USB, Mobile, CD/DVD writer, copy, print, screen capture, external hard disk, upload via http, https, drop box, ftp, telnet."</i></p>	<p>We are accessing our mail using browser, the new mailing system will be netcore. No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above. No change.</p>
	17	4.5	File, folder & removable media level encryption along with the Disk encryption, considering the licenses indicated at 3 above, should be provided.	This feature in Encryption Product feature and hence needs to be removed. This feature in Encryption Product feature and hence needs to be removed.	No change
5	17	4.8	As a Part of Business Continuity Plan BCP, near DR is to be considered. Sync (online / offline) Primary with Near DR.	Do we have to plan for both BCP and Near DR	Bidder has to implement for Near DR.
8	17	4.8	As a Part of Business Continuity Plan BCP, near DR is to be considered. Sync (online / offline) Primary with Near DR	Since this is not a buisness/productivity application what is the need for DR, rather you can create a cluster of database which will not require a complete DR setup & gives the capability of HA.	No change
5	17	4.8	As a Part of Business Continuity Plan BCP, near DR is to be considered. Sync (online / offline) Primary with Near DR.	Do we have to plan for both BCP and Near DR	Bidder has to implement for Near DR.
8	18	4.9	Integration with Arc Sight and other log management solutions	hope they are already installed, fully functional and its SI ready to help us integrate. Bidder expects MDL to co-ordinate with their vendors to meet expectations of our Solution.	The product should be compatible with ArcSight and integration option should be present so that seamlessly integration can be done by bidder with co-ordination with MDL & ArcSight vendor.
20	18	4.9	4.9 Integration with Arc Sight and other log management solutions	Can you be more specific in what do you mean by integration with Archsig? or any other log management? What are you looking for to get from the DLP environment. Would you like to receive the log or the incidents.	Integration means sending the logs seamlessly to the arc sight or any other log management solution for long term stoarge and archival
	20	5.1	The solution should have encryption for encrypting files, folders and drives (on PC & Laptops. The encryption level to be AES 256 bits.	DRM provides this capability. Can bidder provide a 3rd party solution for achieving this ability	Encryption OEM for all type of encryption should be one.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
11	20	5.11	"DLP solution should be able to protect confidential data by automatically enforcing data loss policies; educating users about data security; securing exposed data; and stopping data leaks. data stored in the removable drives should be opened using the password set in an offline mode without any requirement of client in the offline system"	Data can be password protected before copying to USB or CD / DVD. Is automatic encryption a necessity?	Yes
5		5.11	There should be provision for encryption of the data on the file with password protection on the fly when the data is copied to the removable storage drives like CD/DVD & USB drives. The encrypted data stored in the removable drives should be opened using the password set in an offline mode without any requirement of client in the offline system.	This point is favorable to a single OEM and in order to promote fair competition, it should be removed.	No change
6	17	5.11	There should be provision for encryption of the data on the file with password protection on the fly when the data is copied to the removable storage drives like CD/DVD & USB drives. The encrypted data stored in the removable drives should be opened using the password set in an offline mode without any requirement of client in the offline system.	This point is favorable to a single OEM and in order to promote fair competition, it should be removed.	No change
3	21	5.12	Even if the DLP server is down the system should be able to provide the security features as per policy	Can you please elaborate it.	System should be such that once the policies are applied at the server, the same should be downloaded/pushed by the client and in case even if the server is down and not reachable, the client should function as per the policies in the client.
18	17	5.13	The proposed solution should have a provision of recovery of the password incase the user forgets the password. The recovery of the password should be only through the system setup installed in MDL.	Please clarify what all installed systems at MDL are expected to be used for the password recovery. This is a very open statement to be complied by any OEM. Hence, it is requested and recommended to be removed.	Password recovery limited to encrypted file only.
3		5.13	5.13 The proposed solution should have a provision of recovery of the password incase the user forgets the password. The recovery of the password should be only through the system setup installed in MDL.	IS this Query raised for Encryption Password or Windows Password?	Encryption password.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
6		5.13	The proposed solution should have a provision of recovery of the password incase the user forgets the password. The recovery of the password should be only through the system setup installed in MDL.	<p>Please clarify what all installed systems at MGL are expected to be used for the password recovery.</p> <p>This is a very open statement to be complied by any OEM.</p> <p>Hence, it is requested and recommended to be removed.</p>	Password recovery limited to encrypted file only.
	21	5.13	The proposed solution should have a provision of recovery of the password incase the user forgets the password. The recovery of the password should be only through the system setup installed in MDL.	It's the Encryption feature not DLP , Can we use a 3rd party required. Optionally if DRM is being purchased then do we drop the ability for encrypting all files?	Encryption OEM for all type of encryption should be one.
13	17	5.3	<p>Communication channels of Data in MDL through which data flow to be restricted:</p> <p>c. E-mail (Webmail & Fat Clients on Windows and Linux machines)</p> <p>d. Mobile</p>	<p>Point C and D are specific to single OEM, and hence, incase Mazagon Dock does not necessarily need restrict the data flow through eMail client and Mobile, hence, it is requested to amend the statement to as follows:</p> <p>"Communication channels of Data in MDL through which data flow to be restricted</p> <p>a. USB drives</p> <p>b. CD/DVD (optical drives)</p> <p>c. Bluetooth</p> <p>d. Print</p> <p>e. Web Portals having data upload facilities like social networking sites, blogs etc (http & https based)</p> <p>f. ftp and data sharing & IM apps"</p>	Mobile DLP is not required. But data should not be leaked thru connecting mobile to computers.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
3		5.3	Communication channels of Data in MDL through which data flow to be restricted: c. E-mail (Webmail & Fat Clients on Windows and Linux machines) d. Mobile	Point C and D are specific to single OEM, and hence, incase Mazagon Dock does not necessarily need to restrict the data flow through email client and Mobile, hence, it is requested to amend the statement to as follows: <i>"Communication channels of Data in MDL through which data flow to be restricted</i> <i>a. USB drives</i> <i>b. CD/DVD (optical drives)</i> <i>c. Bluetooth</i> <i>d. Print</i> <i>e. Web Portals having data upload facilities like social networking sites, blogs etc (http & https based)</i> <i>f. ftp and data sharing & IM apps"</i>	No Change
4		5.5	The Functional requirements of the Data Loss/Leak Prevention solution are: 5.5.5 Capability to Monitor all traffic flowing out of the Network, irrespective of Policies being in place or not.	Point 5.5.5 refers to an open clause for the policies to be in place or not, that is typically not a standard clause to be met by almost all the OEMs. Hence, it is requested for this specific point to be removed.	Will be removed
2		5.7	5.7 The solution is required to monitor all relevant data leaving the Network and be able to create policy for protection of the same.	Is this mean that DLP should automatically create policies itself?	Policies to be manually configured, but the protection & monitoring should be automatically.
4	21	6.3	The vendor shall bring their licensed data recovery software and all efforts to recover the data from the failed hard disk have to be carried out.	Which licenses we are refering to?	As per policies, the hard disk are not allowed to take out from the MDL, hence data recovery within the MDL premises will be the responsibility of bidder.
	21	6	NA	Please list the other software that MDL needs to install on the machine(Antivirus etc.)	Software related to DLP for the Internet facing machines only.
	21	6	NA	Who will install the other Software on the Machine	Bidder will do installation.
	21	6	NA	Is there a MDL information Security policy that would need to be adhered while setup of the System?. Please provide details	Yes there are security policices and guidelines to be adhered to like password policy, DR policy, backup policy etc.
1		6.1	The hardware at primary and Near DR shall be provided by MDL	provision one more Server	If any hardware, s/w required, then the bidder has to include this as a part of solution.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
1	21	6.3	The Hardware (Server) of HP / Dell / Fujitsu / Cisco / Hitachi make & software (DLP, O/S, Databases and any other software) for the DLP setup for the Internet machines supply & installation is bidder's scope. Rack mounted server should be provided. Intel xeon with minimum dual CPU with 8 cores per CPU, 256GB RAM and 5TB SSD Hard disk in the rack mounted server with mounting rail kit. Bidder to do Fitment of Rack server in existing rack.	Hardware requirement depends on the solution proposed. The Hardware asked for may be oversized or undersized.	The hardware envisaged is the minimum spec required. The bidder has to size the hardware according to its proposed solution. Higher configuration is expected from the bidder, if the hardware requirement is higher.
1	21	6.3	The Hardware (Server) of HP / Dell / Fujitsu / Cisco / Hitachi make & software (DLP, O/S, Databases and any other software) for the DLP setup for the Internet machines supply & installation is bidder's scope. Rack mounted server should be provided. Intel xeon with minimum dual CPU with 8 cores per CPU, 256GB RAM and 5TB SSD Hard disk in the rack mounted server with mounting rail kit. Bidder to do Fitment of Rack server in existing rack.	Hardware requirement depends on the solution proposed. The Hardware asked for may be oversized or undersized.	The hardware envisaged is the minimum spec required. The bidder has to size the hardware according to its proposed solution. Higher configuration is expected from the bidder, if the hardware requirement is higher.
	22	7	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	Please confirm if we are to include or drop SAP integration,DMS integration	No SAP Integration.
	22	7	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	Please confirm version fo SIEM and availability of API/ Support for the same from the give OEM. Has MDL purchased relevant service from SIEM for the project	The Logger model is ArcSight 3505. The product proposed DLP should have seamless Integration with the SIEM

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
	22	7.1	for endpoint, network (100 server nodes to be installed on a virtual environment), encryption at file, folder & removable media & discovering of sensitive, confidential data for LAN setup (including software, operating system, Database licenses) for 2500 nos devices and 250 nos drive/disk encryption considering the primary,	<p>The protection at gateway levels provides protection for sensitive data leaked through network channel (HTTP, HTTPS and SMTP) etc.</p> <p>As there is only endpoints requirement, please suggest if DLP is required at gateway level for Web (HTTP, HTTPS) and Email (SMTP) channel to protect data leaks at network Level apart from endpoints.</p>	<p>There is a requirement at the endpoint level as well as Network Level for web and email as well. The Licenses at 7.100 to be read as follows</p> <p>7.100 Data Loss/Leakage prevention Software for Endpoint, network, Email, encryption at file, folder & removable media & discovering of sensitive, confidential data for LAN setup (including software, operating system, Database licenses) considering 2500 nos devices, 100 server nodes on Linux, and 250 nos drive/disk encryption considering the primary, Near DR site and for Internet machines setup.</p>
6	22	8.1	Bidder has to carry out detailed DFA by consultant, experienced in this area and CISA certified by coordinating with various people, stakeholders / departments, processes and prepare the Data Flow Analysis (DFA), information classification, business & technical requirement and the Policies to be implemented. Deliverable will be final sign off from stakeholders, DFA, information classification policies, best practices for storage of data across organization, DLP security Policies to be implemented.	Requesting you to change it to-DFA should be carried out by OEM in consultation with Bidder.	Instead DFA by CISA certified, the DFA to be done only by OEM. Confirmation from the OEM to be submitted with the technical bid.
13	23	9.5	Customization: Selected bidder shall customize the system as per the requirements of the MDL without any additional cost to the MDL. Customization of the solution would be treated as complete on successful User Acceptance Test. The MDL team shall be included in the process so that they are able to understand the details of the system and process.	Proposed solution would be a standard product. Bidders role is to configure this product as far as the features support. Any customisation or feature enhancement is out of scope of the bidder.	Instead of Customization, treat it as a configuration.
8	23	9.5	Customization: Selected bidder shall customize the system as per the requirements of the MDL without any additional cost to the MDL. Customization of the solution would be treated as complete on successful User Acceptance Test. The MDL team shall be included in the process so that they are able to understand the details of the system and process.	Proposed solution would be a standard product. Bidders role is to configure this product as far as the features support. Any customisation or feature enhancement is out of scope of the bidder.	Instead of Customization, treat it as a configuration.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
	23	9.5	Customization: Selected bidder shall customize the system as per the requirements of the MDL without any additional cost to the MDL. Customization of the solution would be treated as complete on successful User Acceptance Test. The MDL team shall be included in the process so that they are able to understand the details of the system and process.	Please elaborate on customizations that MDL foresees for this project	Instead of Customization, treat it as a configuration.
14	23	10.3	The DLP setup to be installed such that it shall cover all the three active directory domains In MDL in the same setup.	Will the central DLP server deployed be able to communicate with each of the AD servers?	Yes
15	23	10.3	The DLP setup to be installed such that it shall cover all the three active directory domains In MDL in the same setup.	Will the central DLP server deployed be able to communicate with each of the AD servers?	Yes
	23	10.3	The DLP setup to be installed such that it shall cover all the three active directory domains In MDL in the same setup	Please provide the details and architecture for the 3 AD domains. Do the 3 Active directory systems speak with each other. This information is critical as it would help in ascerting if we need to setup multiple instances of the DLP system. It would also help us decide if we need additional hardware for this project	3 AD can communicate with each other, but right now these are 3 separate AD and no connection with each other for the purpose of authentication.
	23	10.3	The DLP setup to be installed such that it shall cover all the three active directory domains In MDL in the same setup	Number of the AD are mentioned 3 are they have trust or all 3 are in Isolations	3 ADs are in isolation and they do not have trust relationship
15	23	10.4	The management of all the three AD domains to be separate and should be carried out by the respective system administrators	Is the bidder responsible for managing Active Directory too?	No
16	23	10.4	The management of all the three AD domains to be separate and should be carried out by the respective system administrators	Is the bidder responsible for managing Active Directory too?	No
	23	10.5	The bidder should study the MDL's data security requirements and configure the classification rules in the system as per the MDL's security requirements	Please share information if this policy would overrule the DFA policy that would be created by the study	The DFA policy shall supplant the existing Security Policy by adding the Data Classification aspects to the existing security policy
	23	10.5	The bidder should study the MDL's data security requirements and configure the classification rules in the system as per the MDL's security requirements	Classification will be done by bidder based on the DFA scope. Is MDL looking for a classification tool as well. Some overlap would be provided by the DRM tool by default	The tools required for carrying out the DFA as well as implementation is in bidders scope.
16	23	10.6	The bidder should install agent in all the clients (PCs, servers, workstations and Laptops) in the organization.	What OS versions are being used in MDL?	Windows client (Vista to 10.0), Windows Servers (2008, 2012, 2016)
9	23	10.6	The bidder should install agent in all the clients (PCs, servers, workstations and Laptops) in the organization.	What OS versions are being used in MDL?	Windows client (Vista to 10.0), Windows Servers (2008, 2012, 2016)

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
	23	10.6	The bidder should install agent in all the clients (PCs, servers, workstations and Laptops) in the organization.	Please confirm information if MDL has a deployment tool configured for all 3 Active Directory	The bidder has to use the native capability of the AD like the Group policies to install the agents on the clients
	23	10.8	A separate setup for the internet facing machines to be installed such that the DLP policies can be configured for the Internet facing machines in MDL. The hardware, software and databases licenses to be supplied by the bidder	Please confirm if we need to have 3 separate instances for each of the AD setup. Please share if the bidder needs to provide exact same hardware and software setup for all instances of the deployment across all 3 AD locations.	Based on the product proposed the bidder has to work out, how the 3 Active directories can be integrated in the solution. The details should be included as part of the Technical bid.
	24	10.8	The setup to be configured such that the policy to be deployed on the internet client over the Internet by the DLP Server.	Please elaborate "Over the internet". Are we having different machines which would be available with Mobile Users?	MDL is providing Internet access to users on standalone Internet Machines not connected to the LAN. The Internet facing setup of DLP to be deployed such that these internet machines should be able to communicate to the Server over the Internet itself.
	25	11.1	Absenteeism of Resident engineer will be penalized on per day basis as given in Penalty Calculation clause	In case of death, injury, illness, otherwise becoming unfit to continue as Resident Engineer request to drop penalty	No change
	25	11.11	It is the responsibility of the bidder to manage/configure the primary, near DR and for the Internet Facing standalone machines of the system and maintain the same during the contract period.	Request to please provide setup and support details of the Primary and near DR details. Request to provide necessary travel, food, stay and ensure co-ordination with team responsible for Near DR and DR	This is post implementation. The bidder to support the DLP setup implemented by the bidder. The Primary & Near DR is within the MDL campus at Dockyard Road. Provision of travel, food, stay will be a bidder's responsibility. Bidder is responsible for both the setup at Primary & near DR for DLP solution.
17	24	11.2	All the items (software and Hardware at Primary, Near DR and Internet facing setup) should be under comprehensive Onsite Warranty for period of 3 years; Warranty of the respective phase shall start after successful the installation, implementation, classifying the sensitive/confidential data along with the stake holders and formulating the policy at primary and near DR and Internet setup, implementation of reports and alerts in the system. Maintenance of equipment shall be responsibility of the bidder.	Product licences and warranty start from the day the licences are issued and cannot start post implementation	The product warranty shall start from the date of Implementation and final sign off only.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
18	24	11.2	All the items (software and Hardware at Primary, Near DR and Internet facing setup) should be under comprehensive Onsite Warranty for period of 3 years; Warranty of the respective phase shall start after successful the installation, implementation, classifying the sensitive/confidential data along with the stake holders and formulating the policy at primary and near DR and Internet setup, implementation of reports and alerts in the system. Maintenance of equipment shall be responsibility of the bidder.	Product licences and warranty start from the day the licences are issued and cannot start post implementation	The product warranty shall start from the date of Implementation and final sign off only.
12		11.3	By way of Quarterly (end of each quarter) running account (after expiry of Guarantee/Warranty) bill per item / activity basis prepared by contractor and certified by the Executives in the rank of CM & above from User department and against the submission of documents such as invoices, guarantee/ training attendance sheet etc. as per the Order / Contract terms between 25 to 30 days with submission of requisite documents as mentioned below: - Invoice documents in Triplicate. - Attendance sheet duly signed by Resident Engineer & MDL User dept Executive in the rank of CM. - Monthly service Report - Work completion Certificate from MDL User dept certified by Executive in the rank of CM & above.	Paladion would like to negotiate this term.	No change
	24	11.4	The bidder has to provide a resident engineer for support, services, Monitoring, Troubleshooting and configuration of the policies, report generations, tracking of incidents on regular basis etc, for the entire duration of the contract. Working time will be from 9:00 AM to 6:30 PM on week days and on call basis as and required on Saturdays, Sundays & Holidays.	Request to keep the service on holidays chargeable at nominal cost	No change
	25	11.9	Bidder should provide support (onsite only) with response time of 4 hours and resolution time of 48 hours. The down time beyond 48 hours will be penalized on per day basis as given in Penalty Calculation clause.	Request to change this to exclude weekend	No change
11		13	The successful bidder shall submit the performance bank guarantee (PBG) for the 10% of the order value for item no. 100, 200, 300 & 400 excluding Duties and Taxes in the form of DD /Pay Order/ Bank Guarantee in favour of Mazagon Dock Shipbuilders Ltd, Mumbai.	Paladion would like to negotiate this term.	No change

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
1	25	14	100% payment of the set up excluding AMC & Resident Engineer charges will be made on the receipt of PBG mentioned below and after successful go live of the solution.	As per the new GST norms if the payment is not cleared in a stipulated time frame the customer cant claim a setoff against GST.	Yes. It is known.
7		14.1	No advance payment will be made.	Paladion would like to negotiate this term.	No change
8		14.5	Penalty Calculation	Penalty terms	No change
2	11	15.6	In case, MDL is unable to avail ITC, supplier/contractor at their own cost shall rectify the shortcoming in the returns to be filed immediately thereafter. Further, if the ITC is delayed/ denied to MDL / reversed subsequently as per GST Laws due to non/ delayed receipt of goods and /or services and / or tax invoice or expiry of timelines prescribed in GST Laws for availing ITC, non-payment of taxes or non-filing or returns or any other reason not attributable to MDL. Supplier/Contractor shall pay any loss of amount along with interest and penalty on MDL under GST Laws for the number of days the ITC was delayed. If the short coming is not rectified by supplier/ contractor and MDL ends up in reversal of credit and / or payments, supplier/ contractor is fully liable for making goods all the loss incurred by MDL. MDL reserves right to recover any interest, penalty or loss from any amount due to Supplier/ Contractor or otherwise.	As per the RFP clause the implementation timelines mentioned as 16 weeks, till that time payment will not be cleared. How will MDL claim the setoff against GST without clearing the payment	Only on completion of entire scope of work, bidder should raise the invoice, even for hardware.
	13	24	Resident Engineer absenteeism ** **Penalties on the event of absenteeism of Resident Engineer, if any shall be calculated for every quarter and recovered from the Resident Engineer charges of that quarter.	In case of death, injury, illness, otherwise becoming unfit to continue as Resident Engineer request to drop penalty	No change
	14	26.2	Vendor should carry out all the configurations and install all the patches/upgrades and carry out any other relevant activity during the period as per MDL's requirements for completion of the Project.	Request to confirm the scope to the deployment and implementation of the DLP solution	It is mentioned in this tender.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
13	9	31	<p>11. TERMS OF PAYMENT:</p> <p>11.2 For Supply Items: Tender Item 100, 200 & 300 Payment for the value of supplies after successful commissioning & acceptance of system by MDL, as reduced by any deductibles and/or the amount leviable towards liquidated damages, if any and after including GST as may be payable through RTGS/NEFT between 25 to 30 days after receipt/ completion of followings:</p> <ul style="list-style-type: none"> - Complete set of the items / Equipment, spares through GRS. - Successful installation, configuration, testing and commissioning of items at all locations. - Original Invoice documents in Triplicate. - Guarantee/Warranty certificate as per Tender/order. - Work completion Certificate from MDL User dept certified by Executive in the rank of CM & above. - Undertaking of Authenticity for IT Products supply from OEM as per format. - Technical documentation & Reports/deliverables as per scope in requisite sets. 	<p>Request to revise the payment term as below:</p> <p>11.2 For Supply Items: Tender Item 100, 200 & 300 : On delivery : 90% On successful installation & commissioning: 10%</p>	No change
14	9	31	<p>11. TERMS OF PAYMENT:</p> <p>11.3 For Service: Tender Item 400 & 500 : AMC & Resident charges will be paid quarterly after completion of the quarter.</p>	Request to revise the payment term from quarterly to monthly	No change
15	28	31	Rate Sheet for buyback	<p>Please suggest, if Bidder does not want to buy back below line item and what would be the impact of the same on commercial evaluation. IBM netfinity 5500 server without hard disk and in as in condition.</p>	No change. This is must condition to qualify and is a part of completion of final implementation activity.
16	12	31	16. भार लाने का मापदंड LOADING CRITERIA	We suggest that loading criteria be dispensed with for payment term, commercials and LD	No change
17	13	31	20. पQR नधा QRत नुकसान LIQUIDATED DAMAGES	We request deletion of this clause. The Bidder will employ commercially reasonable efforts, to meet delivery dates	No change
18	13	31	24. टकना दंड DOWNTIME PENALTY:	We request deletion of this clause.	No change
2	27	300	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	What integration is required with SAP?	SAP word removed

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
1	27	300	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	What integration is required with SAP?	SAP word removed
3	2, 28	600	Buyback - IBM Netfinity 5500 server	Buyback would be specific to vendors dealing in refurbished servers and is not relevant to DLP scope	No change. The bidder has to quote for the buyback.
3	2, 28	600	Buy back - IBM Netfinity 5500 server	Buyback would be specific to vendors dealing in refurbished servers and is not relevant to DLP scope	No change. The bidder has to quote for the buyback.
2	2, 28	600	Buy back - IBM Netfinity 5500 server	Buyback would be specific to vendors dealing in refurbished servers and is not relevant to DLP scope	No change. The bidder has to quote for the buyback.
9		12A	The successful bidder shall submit Security Deposit for an amount of 5% on the value of the contract/ order excluding Taxes, Duties in the form of DD /Pay Order/ Bank Guarantee in the prescribed format as per Annexure-6 in favour of Mazagon Dock Shipbuilders Ltd., payable at Mumbai within 25 days from the date of Contract.	Paladion would like to negotiate this term.	No change
10		12B	The successful bidder shall submit the security deposit of 5% for the total charges for 2 years maintenance contract value excluding Taxes & duties one month before expiry of warranty (i.e. five years from date of work competition date & acceptance of the system by MDL) in the form of DD /Pay Order/ Bank Guarantee in favour of Mazagon Dock Shipbuilders Ltd.	Paladion would like to negotiate this term.	No change
14	5	3.2 (IV)	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores. One completed order with implementation of setup of minimum 2500 DLP licenses. Order copies & work completion certificates to be appended.	Bidders technical capability to be considered . request you to change the simmlar supplies during 3 years should not be less than Rs. 50 Lakhs instead of Rs.1.60 Crore order value, or consider DLP and Encryption combine PO's of Rs. 1.60 crore also request you to prove the technical capabilities a "Limited Product POC" can be conducted for 1/2 weeks Bidder with an order of 1500 licenses will also have same capabilities to implement the required solution. Request for order of 1500 DLP license instead of 2500	No Change

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
15	5	3.2 (IV)	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores. One completed order with implementation of setup of minimum 2500 DLP licenses. Order copies & work completion certificates to be appended.	Bidders technical capability to be considered . request you to change the simmlar supplies during 3 years should not be less than Rs. 40 Lakhs instead of Rs.1.60 Crore order value, or consider DLP and Encryption combine PO's of Rs. 1 crore also request you to prove the technical capabilities a "Limited Product POC" can be conducted for 1 weeks Bidder with an order of 1000 licenses will also have same capabilities to implement the required solution. Request for order of 1000 DLP license instead of 2500	No change
1	5	3.2 (IV)	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores. One completed order with implementation of setup of minimum 2500 DLP licenses. Order copies & work completion certificates to be appended.	Request you to change this Criteria to ensure that you have this amended to have this amended with DLP & Encryption combined to 1.6 crs as Data protection projects do have encryptprtion and DLP combined orders . Also it is unfair to mention that the values have to be proposed only with same OEM solution as being partners we may work with multiple OEM solutions.	No change
2	5	3.2.iii	Audited / Certified Balance sheet, Profit / Loss account for past 3 years as on 31st March 2017.	Can we submit for past 3 years as on 31st March 2016 ?	No change
3	5	3.2.iv	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores	Do you mean the total value shud not be less than INR 1.6 Crores ?	Yes
	5	3.2.iv	The value of the similar supplies during last 3 years should not be less than Rs.1.60 crores. One completed order with implementation of setup of minimum 2500 DLP licenses. Order copies & work completion certificates to be appended.	Request bidder and OEM to jointly bid for the same	This criteria has to be complied by the bidder only.
7	18	5.3c	E-mail (Webmail & Fat Clients on Windows and Linux machines)	Is support for linux system important? How many linux systems ? Which linux versions, Which Email Clients on Linux?	No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above
9	18	5.3c	Communication channels of Data in MDL through which data flow to be restricted	DLP endpoint will not be deployed on Linux machines.	No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
7	18	5.3c	E-mail (Webmail & Fat Clients on Windows and Linux machines)	Is support for linux system important? How many linux systems ? Which linux versions?	No desktop of Linux only servers are present. Currently 25 nos servers. Red Hat Linux 6.0 and above, Suse Linux 11.0 and above
8	18	5.3d	Mobile	Are you also looking for a Mobile DLP solution or is it that the data should not be copied to mobile devices via USB?	Mobile DLP is not required. But data should not be leaked thru connecting mobile to computers.
5		5.4.4.	5.4.4 The solution should be able to detect and block encrypted and password protected files without reading the encrypted content	It needs to be discussed	No change
10	19	5.5.3	The DLP solution should be able to go beyond known policies and provide audit and analysis (includes mobile) capability on all historic data. Thus, the DLP should safeguard sensitive data and ensure compliance by protecting sensitive data wherever it lives on the network, while saving time and money with centralized deployment, management, and reporting.	Can you please elaborate this point? Are you considering to install DLP on mobiles as well? Are you talking about MTP here?	Mobile DLP is not required. But data should not be leaked thru connecting mobile to computers.
6		5.5.3	5.5.3 The DLP solution should be able to go beyond known policies and provide audit and analysis (includes mobile) capability on all historic data. Thus, the DLP should safeguard sensitive data and ensure compliance by protecting sensitive data wherever it lives on the network, while saving time and money with centralized deployment, management, and reporting.	Need to know does mobile devices also needs to be covered as mentioned in brackets.	Mobile DLP is not required. But data should not be leaked thru connecting mobile to computers.
9	19	5.5.5	Capability to Monitor all traffic flowing out of the Network, irrespective of Policies being in place or not.	Point 5.5.5 refers to an open clause for the policies to be in place or not, that is typically not a standard clause to be met by almost all the OEMs. Hence, it is requested for this specific point to be removed.	Clause removed
22	19	5.5.5	Capability to Monitor all traffic flowing out of the Network, irrespective of Policies being in place or not.	Can you confirm that when you are asking to monitor traffic flowing out of the Network, irrespective of Policies being in place or not, you are referring to the endpoint.	Clause removed
	19	5.6.10	DLP Solution must have Indexed Document Matching to evaluate documents for exact content matches on endpoints in real-time to provide greater control over data use when users are off the network.	Please elaborate	It is one of the way the DLP to detect the sensitive data.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
19	20	5.6.12	DLP Solution should prevent confidential/sensitive files from downloading, copying to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; print screens, communications over email, Instant Messaging (IM), and the Web; printing and cloud storage (e.g., Dropbox) and virtual Citrix® environments.	It should be uploading not downloading	Downloading / Uploading.
7		5.6.12	5.6.12 DLP Solution should prevent confidential/sensitive files from downloading , copying to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; print screens, communications over email, Instant Messaging (IM), and the Web; printing and cloud storage (e.g., Dropbox) and virtual Citrix® environments.	Need to know more details on " prevent confidential / sensitive Files from downloading"	The confidential / sensitive data to be defined out as a part of DFA, and then based on the policies defined the prevention of confidential / sensitive to be carried out.
10	20	5.6.12	DLP Solution should prevent confidential/sensitive files from downloading, copying to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; print screens, communications over email, Instant Messaging (IM), and the Web; printing and cloud storage (e.g., Dropbox) and virtual Citrix® environments.	It should be uploading not downloading	Downloading / Uploading.
8		5.6.18	5.6.18 DLP Solution should provide broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the flexible response feature, such as applying encryption to a file using the endpoint encryption flex response.	Need More infirmation on the point " Quarantining or relocating data"	to be removed
10	19	5.6.2	DLP solution should be able to protect confidential data by automatically enforcing data loss policies; educating users about data security; securing exposed data; and stopping data leaks.	What is meant by automatic policy enforcement?	This means the policies formulated shall categorise and protect the data based on the data classifications and automatically the relevant security parameters to be applied.
11	20	5.6.20	DLP Solution should monitor data being copied and pasted from the clipboard to prevent confidential/sensitive data from being pasted to specific application.	What are these specific applications mentioned herein?	The data which is marked for the confidential / sensitive should be monitor being copied and pasted from the clipboard.
12	22	7 - 100	100 server nodes to be installed on a virtual environment	Who has to provide the virtual environment ?	To be read as 100 servers installed on virtual machine on linux, which will be subjected to network DLP scanning.

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
2	22	7 - 300	One time Implementation cost of Data Loss/Leakage prevention solution (It should include DFA, implementation of hardware & software, customization, Integration with MDL email, SAP, Arc Sight SIEM etc)	What integration is required with SAP?	Not required
12	22	8.1.1	Step 1 Data Flow Analysis (DFA) – Bidder has to carry out detailed DFA by consultant, experienced in this area and CISA certified by coordinating with various people, stakeholders / departments, processes and prepare the Data Flow Analysis (DFA), information classification, business & technical requirement and the Policies to be implemented. Deliverable will be final sign off from stakeholders, DFA, information classification policies, best practices for storage of data across organization, DLP security Policies to be implemented.	How many departments? No of processes and sub processes for each department?	Approx. 15 departments / functions & about 6 processes for each departments / functions.
	22	8.1.1	Step 1 Data Flow Analysis (DFA) – Bidder has to carry out detailed DFA by consultant, experienced in this area and CISA certified by coordinating with various people, stakeholders / departments, processes and prepare the Data Flow Analysis (DFA), information classification, business & technical requirement and the Policies to be implemented. Deliverable will be final sign off from stakeholders, DFA, information classification policies, best practices for storage of data across organization, DLP security Policies to be implemented.	Please provide guideline about the Service that need to be adhered to while execute the	
	22	8.1.1	NA	The DFA process involves study and access to confidential documents. If MDL allows bidder to involve 3rd Party consultants who are CISA qualified for this activity then the internal working of the enterprise would be exposed to the consultant. Suggest to ensure that bidder has a minimum of 8 fulltime CISA qualified personnel to ensure that work is done in the stipulated timeframe.	Instead DFA by CISA certified, the DFA to be done only by OEM. Confirmation from the OEM to be submitted with the technical bid.
	23	9.2.4	Mutually agreeable Acceptance Criteria	Provide guidance if any on this front	
13		NA	NA	Paladion shall consider following activities to be out of scope for resident engineer:	No change

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
	28	NA	IBM Netfinity 5500 server without hard disk and in as is condition.	Please provide Manufacturing year, ram, CPU, service record. Does the machine have a Windows License that it was purchased with and any other license that was bundled with the machine?	This is not in working condition. No licenses are bundled with it.
	NA	NA	NA	Please provide Minimum Technical Qualification Criteria details for clearing the round	All the PQ criterias to be filled along with the compliance to the Technical Scope
	NA	NA	NA	What is the minimum criteria for Technical qualification?	All the PQ criterias to be filled along with the compliance to the Technical Scope
	NA	NA	NA	How many machines and users are configured at each Active directory	Machines are around 2500 nos including stores.
	NA	NA	NA	How many machines and users exist at Anik and Sewri Locations	Machines are around 2500 nos including stores.
7			Eligibility	Requesting you to add a clause- All DLP end encryption solutions should be from single OEM	No change.
				Deployment of agents will be handled by Desktop Support staff.	No change
				Monitoring of DLP incidents.	No change
				Data Classification	No change
1			What is the difference between comprehensive warranty and AMC		Only payment terms are different.
2	16		Annexure 12 – Undertaking of Authenticity for IT Products Supplies. Our legal team has made certain changes as per the standard terms of Symantec. Request you to please review the same and share if this is acceptable to mazgaon dock	Deviation sought	The deviation sought, will be taken dealt after the bid submission.
				In case of damage due to MDL negligence it is proposed that that MDL would provide replacement for the same and waiver of penalty	No Change
				There are multiple Setup mentioned for the Intranet and Internet , How many machines will be there in each setup.	2350 nos in LAN and 150 nos in Internet
				As per understanding LAN users will be use the Email and Endpoint Channel ?	Yes. Email, Endpoint and Web
				Internet Users will be used for the Web and Endpoint DLP Solution ?	Yes
				Will the solution also be required for Near DR and DR , for the individual Setup ?	For Primary & Near DR
	1. M/s. Doyen				
	2. M/s. Hitachi Systems Micro Clinic Pvt Ltd.				
	3. M/s. Valuepoint Techsol				

Sr.	Page n	clause	Existing Clause Details	Clarification Sought	MDL Reply
	4.		M/s. Rah Infotech (P) Ltd		
	5.		M/s. AVI Infotech		
	6.		M/s. Paladion		
	7.		M/s. Yonit Systems		
	8.		M/s. Atos India Pvt. Ltd.		
	9.		M/s. Symantec		
	10.		M/s. Polestar Technologies		
	11.		M/s. Deloitte		