No.E-Gov/New Project(1).2015-Vol-I

Dated : 30.11.2017

CORRIGENDUM-III - TO TENDER NOTICE No. DGS/E-GOV/NP(1)/2015-VoI-1

Subject :- **Corrigendum-III on Request for Proposal (RFP) for Selection of System integrator for e-Governance solution and transformation of Directorate General of Shipping, Govt. of India.**

In continuation of the Tender Notice No.DGS/E-GOV/NP(1)/2015-VoI-1 dated 17.10.2017 and corrigendum's dated 17.11.2017 & 27.11.2017 on the above subject. Amendment of clause & clarification on the above RFP.

[Deependra Singh Bisen]
Asstt. Director General of Shipping

Encl: Corrigendum-III

CORRIGENDUM 3 TO
THE RFP FOR SELECTION OF SYSTEM INTEGRATOR FOR EGOVERNANCE SOLUTION AND IT TRANSFORMATION OF DIRECTORATE GENERAL OF SHIPPING, GOVT OF INDIA

CONTENTS

1   Amendment of Clauses

Kindly refer to the table below for amended clauses and sections

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
1.	I	10.3 (A10)	97	Summary of Commercial Proposal Scanning and Digitization Services	Refer to Amended Sections 2.1 (A)
2.	Annexure	Annexure 2	78, 79, 80, 88-100	Technical Specifications 1. Desktop 2. Laptop 8. Enterprise Management System	Refer to Amended Sections 2.1 (B)

2   Clarifications

Sr. No.	Clarification
1.	Bidder is supposed to Integrate with the existing e-mail system of DGS. Bidder is not required to provide a new solution.
2.	If any equipment is provided by the cloud service provider as a service then bidder is not mandated to submit the MAF.

2.1 Amended Sections of RFP Volume I

A. Comp1: Summary of Commercial Proposal

The Summary for Scanning & Digitization will be read as follows

A10: Scanning and Data Digitization services

Data Entry

Sr. No.	Description	Quantity (A10.1)	Rate (A10.2)	Period (A10.2.1)	Total Price (Rs.) A10.3 =(A10.1 * A10.2*A10.2.1)
1.	Data Entry operators (minimum 5 resources)				

Total data entry fields (approximately)	**6,00,00,000**

Scanning & Digitization

Sr. No.	Description (Size of the document)	Quantity (A10.4)	Rate (A10.5)	Total Price (Rs.) A10.6 =(A10.4 * A10.5)
1	A0	1,10,000		
2	A1	25,000		
3	A2	15,000		
4	A3	-		
5	A4	98,50,000		
6	Legal			
	TOTAL (A10.7)			

Total pages to be scanned	**1,00,00,000**

Tax: Against A10 component

Subtotal (A10.3) and (A10.7)	Tax	Tax rate	Tax amount	Total A10 = (A10.3 + A10.7 + Tax amount)
	CGST			

	SGST			
	IGST			
	Any other tax			
Total (in Figures) (A10)				
Total (in Words) (A10)				

B. Annexure 2 – Technical Specifications

Technical Specification for HDD in Desktop & Laptop and Enterprise Management System in the Annexure 2 will be read as follows

1.DESKTOP					
#	**Nature of Requirement**	**Minimum Requirement Description for Desktop**	**Compliance (Y/N)**	**Reasons for Deviation (if any)**	**Details**
1	CPU	Intel or AMD			
2	Processor	Intel **Core i5** or Higher and for AMD A10 CPU or better			
3	CPU Speed	Minimum 3 GHz or higher			
4	Chipset	Intel H81 or Higher for A75 Chipset or higher			
5	Cache Memory	Minimum 3 MB or higher			
6	Memory	8 GB DDR3 RAM Min. 667MHz Upgradable up to 16GB			
7	HDD	500 GB			
8	Operating System	**Preloaded with latest windows 8 or higher professional 64 bit OS.**			
9	Monitor	Minimum 18.5" or higher wide monitor with TCO5 certification: 1366 X 768			
10	Keyboard (Bilingual , Hindi and English)	Multimedia Keyboard from same OEM			

11	Mouse	Two Button Optical Scroll Mouse			
12	Optical Drive	DVD writer and the corresponding software			
13	Ports	Min. 4 USB, 1 Serial, 1 Parallel, PS/2 (For Keyboard & Mouse)			
14	Certification	TCO 05 certified Monitor; Energy star 5.0 or above/ BEEstar certified; 80plus certified power supply; The Restriction on Hazardous Substance Directives (RoHS) for environment safety.			
15	Anti-Virus	Preloaded antivirus along with patches and updates for 5 years.			
16	Warranty	Comprehensive 5 years onsite warranty			
17	**Software**	**MS- Office Latest Version**			

2.LAPTOP					
#	**Nature of Requirement**	**Minimum Requirement Description for Laptop**	**Compliance (Y/N)**	**Reasons for Deviation (if any)**	**Details**
1	Processor	Intel Core i5 or Equivalent			
2	Speed	Minimum 3 GHz or higher			
3	Memory	4 GB DDR3 RAM Min. 667MHz Upgradable up to 8GB			
4	HDD	250 GB			

6	Operating System	**Preloaded with latest windows 8 or higher professional 64 bit OS**			
7	Display	Minimum 12" or higher wide display with TCO5 certification: 1366 X 768 HD LED Anti-Glare Display			
8	Keyboard (Bilingual , Hindi and English)	Min. 104 Keys OEM Mechanical Key Board or TVSE Gold or Equivalent			
9	Anti-Virus	Preloaded antivirus along with patches and updates for 5 years.			
10	Warranty	Comprehensive 5 years onsite warranty			
11	Networking	Ethernet Port: 1, Ethernet Type: 10/100/ 1000, WiFi Type: 802.11b/g/ n, LAN connectivity			
12	Standard Battery	Upto 9 hours back-up, 6 cell including Charger			
13	Additional features	Built-in HD Camera, Microphone, Digital Media Reader slot, Light weight, Bluetooth, Speakers, Touchpad with Track Point			
14	**Software**	**MS - Office Latest Version**			

8. ENTERPRISE MANAGEMENT SYSTEM					
#	**Nature of Requirement**	**Minimum Requirement Description for EMS**	**Compliance (Y/N)**	**Reasons for Deviation (if any)**	**Details**
1	Basic Requirement	Solution should provide for future scalability of the whole system without major architectural changes.			
2	Basic Requirement	Should be SNMP compliant.			

3	Basic Requirement	Filtering of events should be possible, with advance sort option based on components, type of message, time etc.			
4	Basic Requirement	Should support Web / Administration Interface.			
5	Basic Requirement	Should provide compatibility to standard RDBMS.			
6	Basic Requirement	Solution should be open, distributed, and scalable and open to third party integration.			
7	Application Performance Management	End to end Management of applications (J2EE/.NET based)			
8	Application Performance Management	Determination of the root cause of performance issues whether inside the			
9	Application Performance Management	Java / .Net application in connected back-end systems or at the network layer.			
10	Application Performance Management	Automatic discovery and monitoring of the web application environment			
11	Application Performance Management	Ability to monitor applications with a dashboard.			
12	Application Performance Management	Ability to expose performance of individual SQL statements within problem transactions.			
13	Application Performance Management	Monitoring of third-party applications without any source code change requirements.			
14	Application Performance Management	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.			
15	Application Performance Management	Storage of historical data is for problem diagnosis, trend analysis etc.			
16	Application Performance Management	Monitoring of application performance based on transaction type.			
17	Application Performance Management	Ability to identify the potential cause of memory leaks.			
18	Reporting	Should able to generate reports on predefined / customized hours.			
19	Reporting	Should be able to present the reports through web and also generate "pdf" / CSV / reports of the same.			
20	Reporting	Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.			
21	Reporting	Should provide information regarding interface utilization and			

		error statistics for physical and logical links.			
22	Reporting	Should create historical performance and trend analysis for capacity planning.			
23	Reporting	Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.			
24	Reporting	Should have capability to exclude the planned-downtimes or downtime outside SLA.			
25	Reporting	Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.			
26	Reporting	Should be able to generate the reports for Server, Application.			
27	Reporting	Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.			
28	Availability Reports	Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis			
29	Availability Reports	Trend Report			
30	Availability Reports	Custom report			
31	Availability Reports	MTBF and MTTR reports			
32	Performance Reports	Device Performance – CPU and Memory utilized			
34	Performance Reports	Interface errors			
35	Performance Reports	Server and Infrastructure service statistics			
36	Performance Reports	Trend report based on Historical Information			
37	Performance Reports	Custom report			
38	Performance Reports	SLA Reporting			
39	Performance Reports	Computation of SLA for entire DC/DR Infrastructure			
40	Performance Reports	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports.			
41	Data Collection	For reporting, required RDBMS to be provided with all licenses.			
42	Data Collection	Should have sufficient Storage capacity should to support all reporting data			

43	Integration	Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.			
44	Integration	Should be able integrate with Helpdesk system for incidents.			
45	Integration	Should be able to send e-mail or Mobile –SMS to pre-defined users for predefined faults.			
46	Integration	Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.			
47	Network Management	The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.			
48	Network Management	It should proactively analyze problems to improve network performance.			
49	Network Management	The Network Management function should create a graphical display of all discovered resources.			
50	Network Management	The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display.			
51	Network Management	The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting, and analysis.			
52	Network Management	The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers.			
53	Network Management	Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as emails, etc.			
54	Network Management	It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.			

55	Network Management	The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:			
56	Network Management	Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.			
57	Network Management	File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds.			
58	Network Management	Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.			
59	Network Management	System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.			
60	Network Management	Memory: The System Management function should monitor memory utilization and available swap space.			
61	SLA Monitoring	The SLA Monitoring component of EMS will have to possess the following capabilities:			
62	SLA Monitoring	EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:			
63	SLA Monitoring	Response times of Portal;			
64	SLA Monitoring	Uptime of IT Infrastructure;			
65	SLA Monitoring	Meantime for restoration of services etc.			
66	SLA Monitoring	EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.			
67	SLA Monitoring	The EMS should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the			

		Agency after applying the system of penalties and rewards.			
68	SLA Monitoring	The SLA monitoring component of the EMS should be under the control of the authority that is nominated the client so as to ensure that it is in a trusted environment.			
69	SLA Monitoring	The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability, and integrity.			
70	ITIL based Helpdesk	Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC/DR support framework.			
71	ITIL based Helpdesk	The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.			
72	ITIL based Helpdesk	The web interface console of the incident tracking system would allow viewing, updating, and closing of incident tickets.			
73	ITIL based Helpdesk	The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.			
74	ITIL based Helpdesk	Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.			
75	ITIL based Helpdesk	It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.			
76	ITIL based Helpdesk	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.			
77	ITIL based Helpdesk	It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.			

78	ITIL based Helpdesk	It should be possible to sort requests based on how close are the requests to violate their defined SLA's.			
79	ITIL based Helpdesk	It should support multiple time zones and work shifts for SLA & automatic ticket assignment.			
80	ITIL based Helpdesk	It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.			
81	ITIL based Helpdesk	System should provide a knowledge base to store history of useful incident resolution.			
82	ITIL based Helpdesk	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.			
83	ITIL based Helpdesk	The web-based knowledge tool would allow users to access his / her knowledge article for quick references.			
84	ITIL based Helpdesk	It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities.			
85	ITIL based Helpdesk	Provide seamless integration to generate events/incident automatically from NMS / EMS.			
86	ITIL based Helpdesk	Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.			
87	ITIL based Helpdesk	Allow categorization on the type of incident being logged.			
88	ITIL based Helpdesk	Provide audit logs and reports to track the updating of each incident ticket.			
89	ITIL based Helpdesk	Proposed incident tracking system would be ITIL compliant.			
90	ITIL based Helpdesk	It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.			
91	ITIL based Helpdesk	It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies.			
92	ITIL based Helpdesk	It should be able to log and escalate user interactions and requests.			
93	ITIL based Helpdesk	It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.			

94	ITIL based Helpdesk	It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.			
95	ITIL based Helpdesk	It should provide status of registered calls to end-users over email and through web.			
96	ITIL based Helpdesk	The solution should provide web based administration so that the same can be performed from anywhere.			
97	ITIL based Helpdesk	It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.			
98					
99	Client Management System	The proposed desktop management system should provide single integrated agent for asset management, remote software deployment and remote desktop control.			
100		:			
101	Asset Management System	The proposed Asset Management solution must provide inventory of hardware and software applications on end-user desktops including information on processor, memory, operating system, mouse, key board of desktops etc. through agents installed on them.			
102	Asset Management System	The proposed Asset Management solution must have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs.			
103	Asset Management System	The proposed Asset Management solution must have the capability to export the reports to CSV, HTML and XML format.			
104	Asset Management System	The proposed Asset Management solution must provide the facility for user defined templates to collect custom information from desktops.			
105	Asset Management System	The proposed Asset Management solution must provide facility to recognize custom applications on desktops.			

106	Asset Management System	The proposed Asset Management solution must support administrators to register a new application to the detectable application list using certain identification criteria's (Like executable, Date/time stamp etc.). The new application must be detected automatically from next time the inventory is scanned.			
107	Asset Management System	The proposed Asset Management solution must provide facility for queries and automated policies to be set up and permit scheduling of collecting engines to pick up the data at defined intervals.			
108	Asset Management System	The proposed Asset Management solution must be able to collect WBEM information.			
109	Asset Management System	The proposed Asset Management solution must integrate with the helpdesk solution and allow ticket creation automatically on an event defined in asset management solution. It should also allow manual ticket creation also.			
110	Asset Management System	The proposed Asset Management solution must support Software metering to audit and control software usage where launching of an application can be prevented based on centrally configured number of licenses for an application.			
111	Remote Software Deployment System	It should provide delivery, installation, and un-installation of software (ex. Patches of Anti-virus solution etc.) installed on end-user desktops by software delivery remotely through agents installed on them. It must allow pre- and post-installation steps to be specified if required & support rollback in the event of failure in installing software to end-user desktops.			
112	Remote Software Deployment System	The tool should have the capability to install applications based on interdependencies i.e. to be installed in a particular order.			
113	Remote Software Deployment System	It should support deployment of MSI based packages using drag and drop method.			
114	Remote Software Deployment System	It should perform actual distribution of software remotely, not mere file transfer and manual installation at other end. Automated installation should be possible.			

115	Remote Software Deployment System	It should include a Software packager for creating software packages to be delivered to end-user desktops which uses a snap-shot technology.			
116	Remote Software Deployment System	It should support both push and pull software distribution modes. A catalog/advertisement option of the existing software delivery packages must be provided for end-user to download and install software of his / her choice.			
117	Remote Software Deployment System	Users must be allowed to cancel jobs if they are launched at an inconvenient time. Cancelled jobs must be allowed to be reactivated. Forcing packages onto the computer must also be possible.			
118	Remote Desktop Control Management System	The proposed solution should allow remote control of end-user desktop for facilitating resolution of desktop issues without the need to go to the end-user desktop, through agents installed on them.			
119	Remote Desktop Control Management System	It should provide the capability of taking Remote control of Linux systems also using Views sitting on Windows platform.			
120	Remote Desktop Control Management System	It should provide Windows integrated authentication as well as application based authentication option to choose from for the agent installed.			
121	Remote Desktop Control Management System	It should allow host enabled recording which allows the end user to initiate a recording session.			
122	Remote Desktop Control Management System	It should have the ability to convert the recorded sessions in AVI/WMA format so it can be replayed using commonly available Windows media player.			
123	Remote Desktop Control Management System	Centralized User Management should allow administrators to centrally manage remote control users' and their access rights. Administrators must be able to define preferences and capabilities different users or user groups have, as well as defining which targets they can control.			
124	Remote Desktop Control Management System	It should support Seamless integration with management applications such as helpdesk, asset management and Software delivery.			

125	Remote Desktop Control Management System	It should support remote Reboot & Chat functions between nodes.			
126	Remote Desktop Control Management System	It should provide facility for encrypting the authentication traffic and support AES 256.			