Pre-Bid Queries for NIT No. RECPDCL/TECH/IT Security-GED/e-Tender/2015-16/1518 Dated:04.09.2015
Rate Contract of Supply and installation of IT Security Solution (Hardware and Software)

S. No.	Vendor	Item	Page No. / Clause No.	Parameter	Technical Specifications as per RFP	Queries / Modifications / Changes Suggested	Vendor's Remarks	RECPDCL Remarks
1	CA		Page 14, Sub Section 1.8	Section - 2.1 (Technical specification for Identity and Access Management System)	Certification - The Proposed solution should be certified as "Liberty Interoperable?" And Should be interoperable with other products solution based on SAML 2.0 for the following profiles: 1. Identity Provider 2. Identity Provider Extended 3. Service Provider 4. Service Provider Complete 5. Service Provider Extended 6. ECP 7. Attribute Authority Requester 8. Attribute Authority Responder 9. Authorization Decision Authority Requester 10. Authorization Decision Authority Responder 11. Authentication Authority Requester 12. Authentication Authority Responder 13. POST Binding 14. GSA Profile	What solution thought you planned with this fuctionality? Are you planning for SAML base web single sign on solution? The solution can be in multiple way without SAML.		Proposed solution should be integrated with other products / applications based on SAML 2.0 for profiles mentioed in specifications.
2	CA		Page 13, Section 2.1	Section - 2.1 (Technical specification for Identity and Access Management System)	Technical specification for Identity and Access Management System	How many Number of (Internal users) users will be part of this solution? How many number of (Consumer users) external users will be considered? Are you planning for IDM / SSO solution mentioned for entier GOA subscription list?		Solution should be proposed only for internal users and not for external users (consumers) there will be 1000-1100 internal users which will be a part of this solution.
3	CA		Page 13, Section 2.1	Section - 2.1 (Technical specification for Identity and Access Management System)	Technical specification for Identity and Access Management System	List of Applications and details of the applications to be integrated with SSO or IDM systems. Like Application server, Web server and Database		Common applications will be various SAP modules,microsoft exchange, active directory, SAP BCM and other home grown and custom applications will be finalized at the time of implimentation. Database will be oracle, sybase and SQL.
4	CA		Page 23 - Sub-section 8.5	Section - 2.1 (Technical specification for Identity and Access Management System)	Enterprise Single Sign on - Ability to incorporate Enterprise Single Sign On products to include the provisioning solution within the Thick client single sign-on environment.	Do already have any thick client application and How many of them / also how many users will be using these applications.		This will be a new implemenation of applications, servers, database, network. Common applications to be installed may have thick client for administation. Most of the users out of total user license will be using SSO thick client if required.
5	CA		Page 24 - Sub-section 9.5	Section - 2.1 (Technical specification for Identity and Access Management System)	Synchronization with user information - Ability to load and maintain synchronization with user information from existing human resources and other identity systems, both statically and dynamically.	Required clarifications, as it might create integrity issues.		No changes required, we need syncronization to be done related to user information from human resource application and active directory tools.

6	CA		Page 24 - Sub-section9.1	Section - 2.1 (Technical specification for Identity and Access Management System)	Web-based functionality - Entirely Web-based functionality to allow easy distributed administration on an unlimited scale.	How can be there are unlimited administrations? Or you want to mention unlimited user access		Web based functionality should allow easy administration of software on unlimited scale.
7	CA		Page 32 - Sub-Section 5.6	Section - 2.1 (Technical specification for Identity and Access Management System)	Software change control - A mechanism for controlling software changes during development shall be implemented. This mechanism shall as a minimum ensure that : a) The change is reviewed by appropriate groups prior to authorization, b) Changes are properly authorized prior to implementation, c) All change requests are logged. d) All associated documentation is altered along with the software change. e) Version control records are maintained.	Clarification and further information required.		The scope of this specification is to log the changes done in software / application integrated with IDMS system. These changes shall be reviewd by authorized groups prior to implementation.
8	CA		Page 13, Section 2.1	Section - 2.1 (Technical specification for Identity and Access Management System)	Technical specification for Identity and Access Management System	What are the applications to be integrated with the solution?		Common applications to be installed will be various SAP modules, microsoft exchange, active directory, SAP BCM for call center and other home grown and custom applications will be decided at the time of implementation.
9	CA		Page 13, Section 2.1	Section - 2.1 (Technical specification for Identity and Access Management System)	Technical specification for Identity and Access Management System	How many servers to be integrated with Privilege Identity Management solution? Critical servers and network devices. Please share separate count for servers and network devices / security devices.		Total number of physical servers will be - DC - 47 DR - 33 Total number of virtual servers - 46 Total number of network devices / security devices - 500
10	Megahertz			ANTIVIRUS FOR ENDPOINTS & SERVERS	Solution should have the capability to protec the HTTPS connections by proving connection control	Connection Control prevents banking trojans from sending sensitive information to online criminals. It does this by automatically closing network connections to unknown sites and preventing new ones during business-critical actions such as online banking. You can enable Connection Control to sites that support HTTPS.		Bid will be evaluated as per technical specifications mentioned in tender.
11	Megahertz			ANTIVIRUS FOR ENDPOINTS & SERVERS	Solution should provide the capability to block websites on category basis	Web Content Control enables you to restrict unproductive and inappropriate Internet usage and manage what Web content users are allowed to access from the company network		Bid will be evaluated as per technical specifications mentioned in tender.
12	Megahertz			ANTIVIRUS FOR ENDPOINTS & SERVERS	Solution should provide the capability to provide block the download of the files on the basis of file extension	Web Traffic Scanning Advanced Protection enables you to block certain content from unknown sites, ensuring that employees can work safely and efficiently online.		Bid will be evaluated as per technical specifications mentioned in tender.
13	Megahertz			ANTIVIRUS FOR ENDPOINTS & SERVERS	Solution must have the capability to host the central server on Linux (RHEL,SUSE,CENTOS,Ubuntu,Debian) And Windows server (2008,2012) flavor	Hosting central server on Linux Helps to avoid Microsoft CAL costs as well.		Solution must support the OS mentioned in tender, however we will decide out of mentioned OS to be installed at the time of implementation.

14	Megahertz			ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP	Solution must support the machine learning technology for accurate content analysis	Continuously adapts to detect new types of spam without manual intervention		Bid will be evaluated as per technical specifications mentioned in tender.
15	Megahertz			ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP	Solution must have the the End User Digest facility to release the email seamlessly.	Users can view the list of messages they have in the Quarantine or Incident Queue, and request that the messages are released, or request that the messages are released and the sender of the message be added to a personal Safe Senders list.		Bid will be evaluated as per technical specifications mentioned in tender.
16	Megahertz			ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP	Solution should include Zero-hour threat detection,message tracing	Protects enterprises against new email security threats, such as phishing attacks and viruses as they emerge. This adds an additional layer of security threat assessment and detection over the Spam Detection, Phishing Protection, and Virus Protection layers, providing critical defense-in-depth protection.		Bid will be evaluated as per technical specifications mentioned in tender.
17	Ricoh India			As per RFP page no. 54 Sr.no.3.A Pre-Qualifying Criteria for Bidder	The bidder needs to provide details of at least 3 similar successfully completed projects (meeting any of the three criteria below) in the last 3 (FY 2012-13, 2013-14, 2014-15 and till the date of bid publication) financial years in the following format along with the copy of the completion Certificate. Proof: Contract/LOI/WO/PO along with completion certificate on client letterhead. a. One project covering supply, installation, commissioning and testing of IT security Solutions of equal or more than value of Rs. 1.60 Crore.	Request you to please consider the list price of the mentioned product in a consolidated BOM as per attached reference PO. As per the industry standard, list price of the product is considered, when price bifurcation is not there		As per tender specifications, PO value will be considered for evalaution purpose. In case bidder provides clubbed order, then PO should be accompanied with list of items and list price duly certified by its supplier.
18	AKAL Information Systems Ltd.			Page no 54 Selection-VI of Eligibility criteria	The OEM vendor shall have ISO 9001:2008 and ISO 14001 certifications	ISO 9001:2008 OR ISO 14001 certifications		ISO 14001 to be submitted for hardware OEMs only not for software OEMs.
19	AKAL Information Systems Ltd.			Page no 54 Pre-Qualifying Criteria for Bidder Point 3 Work Order	The bidder needs to provide details of at least 3 similar successfully completed projects (meeting any of the three criteria below) in the last 3 (FY 2012-13, 2013-14, 2014-15 and till the date of bid publication) financial years in the following format along with the copy of the completion Certificate	Can we show the order Consortium with OEM		Consortium and joint venture responses are not allowed, in any case. The WO/PO should be in the name of Bidder who is submitting the bid.