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	CA	Page 16	sub section 2.7	Communicating usage restrictions	A prescribed warning screen shall be displayed immediately after a user successfully completes the logon sequence to any multi user system, server or database. This does not apply when logging onto a PC, which cannot be accessed via any other means, or when logging onto a network where no information is available without further logon (note: the screen should be presented after this further logon). This screen will emphasize the requirement to comply with requirements on usage of computer as laid down by the Purchaser. The screen will require confirmation that the user has understood these requirements prior to proceeding.	Prescribed warning screens would be customized during implementation stage by implementation team where appropriate warning messages will be populated. This specs should not be mentioned in the scope of IAM solution. SI can comply this.		This specs is needed as a part of identity and access management solution. Scope shall be complied with efforts of SI and OEM.
11	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.
12	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.
13	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.
14	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.

15	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.
16	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.
17	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.
18	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.
19	Ricoh India			page 32, 1.3	Firewall appliance should have 16 x 10/100/1000 Gigabit Ethernet interfaces	please add 2 x 10G interfaces		bid will be evaluated as per tender specifications.
20	Ricoh India			1.2	Appliance based Firewall shall have throughput of 5Gbps handling a minimum of 50000 simultaneous session per second & having Gigabit Ethernet interfaces	please increase throughput to 50 Gbps & 280K simultaneous sessions per second		No changes required, capacity planning has already been done based on the servers and no. of consumers.
21	Ricoh India			1.8	Firewall should support 1 Million concurrent firewall sessions	please increase to 10M concurrent firewall sessions		No changes required, bid will be evaluated as per tender specifications.
22	Ricoh India			1.11	It should have 1TB of Total Hard Drive Capacity	Please allow internal / external logging appliance with 1TB disk		It should have 500 GB of total hard drive capacity (internal or external)
23	Ricoh India			2.4	Should have in-built redundancy for storage, if applicable and power	Only for power (remove storage)		system needs to have in built redundancy, bid will be evaluated as per tender specifications.
24	Ricoh India			7.2	Fails open should a Power loss/Ethernet/hardware/software failure occur.	Since IPS is part of Firewall , it will be deployed in NAT mode so please remove fail open		IPS will be independently deployed without integration of firewall. Fail open feature is required in case one or both the IPS is not available.
25	Ricoh India			14.4	Can export reports to other formats. Users should be able to output report data into a variety of different file formats like HTML, PDF, CSV, and Printer -	please remove CSV		CSV format is a requirement for NIDS reporting, same cannot be removed.
26	Ricoh India			Page 22, Section 7-9.21		This specification seems to be ERP/ Oracle Solution quoted for other APDRP projects. These Specification has to be made by ERP/ Oracle application vendor.	Request you to please remove this entire section from the RFP so that we can participate.	System security solution is excluded from the tender, ammendment will be released for excluding the solution.
27	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.

28	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.
29	Symentec	2.4. Technical specification for Antivirus solution		Page 41, clause 2.26	Solution should support Bayesian filtering of mails	It is requested to make this spec vendor neutral. This specs may be rephrased as " Solution should support Bayesian or equivalent filtering of mails.		Solution should support Bayesian or equivalent filtering of mails
30	Symentec	Technical specification		1.20	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.	Sometime system may require reboot and system binaries are changed while upgrading the scanning Engine. It is requested to change the spec to "Should be able to update definitions & scan engine on the fly, without a need stopping of services on servers."		Solution should be able to update definitions and scan engine without a need for reboot the system / servers unless and untill reboot is required by a system for a particular definition or patch distribution.
31	Symentec	Technical specification		1.41	Should enable administrators to select the events that clients forward to their parent servers and those secondary servers forward to primary servers.	There are other alternative in which an Anti-virus can be deployed. It is requested to change the spec to "Should enable administrators to select the events that clients forward to their parent servers and those secondary servers forward to primary servers or alternative architecture which will not have impact on the network bandwith."		Should enable administrators to select the events that clients forward to their parent servers and those secondary servers forward to primary servers or alternative architecture
32	Symentec	Technical specification		2.3	Should enable administrators to use other DNS-based blacklist services (DNSBL), other than just MAPS (Mail-Abuse Prevention Systems, LLC). Should enable administrators to use Services like Reputation Service, SenderID, RBLs, SPF, DKIM other than just MAPS.Should be able to use multiple lists in combination to maximize spam detection based on the various possible sources of spam.	MAPS is normally subscribed by ISP which is nothing but RBL. Different OEM have their own RBLs and solutions can be configured to subscribe to different RBLs. There are other technologies which Symantec uses like DisArm, adaptive reputation and local reputation to block any spam. It is suggested to rephrase the spec to read as "Should enable administrators to use other DNS-based blacklist services (DNSBL), other than just RBLs (Real time black list). Should enable administrators to use Services like Reputation Service, SenderID, RBLs, SPF, DKIM other than just RBLs. Should be able to use multiple lists in combination to maximize spam detection based on the various possible sources of spam."		Should enable administrators to use other DNS-based blacklist services (DNSBL), other than just MAPS (Mail-Abuse Prevention Systems, LLC) / RBLs (Real time black list). Should enable administrators to use Services like Reputation Service, SenderID, RBLs, SPF, DKIM other than just MAPS / (RBLs).Should be able to use multiple lists in combination to maximize spam detection based on the various possible sources of spam.
33	Symentec	Technical specification		2.33	Solution should support spam scanning on PoP3 protocol as well	PoP3 is not possible over SMTP. Request you to remove the spec.		POP3 is an incoming mail protocol, solution should support scanning of spam on this protocol also which is not dependent on SMTP.
34	F Secure	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.	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.

35	F Secure	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	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
36	F Secure	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.	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
37	F Secure	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.	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
38	F Secure	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	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
39	F Secure	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.	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
40	F Secure	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.	Additional functionality can not be incorporated at this stage. Bid will be evaluated as per technical specifications mentioned in tender.	
41	Fortinet	Firewall and NIDS	32	2.3 Technical specification for Firewall and NIDS Solution - Point No -1.2	Appliance based Firewall shall have throughput of 5Gbps handling a minimum of 50000 simultaneous session per second & having Gigabit Ethernet interfaces.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. To cater to such high sessions requirement it is suggested that the Firewall throughput should be increased to 50 Gbps and at least 250K new sessions per second		No changes required, capacity planning has already been done based on the servers and no. of consumers. Based on the inputs appliance based firewall with throughput of 5 Gbps and 50000 simultaneous sessions will suffice.	
42	Fortinet	Firewall and NIDS	32	2.3 Technical specification for Firewall and NIDS Solution - Point No -1.3	Firewall appliance should have 16 x 10/100/1000 Gigabit Ethernet interfaces	Today 1G have already peaked and 10G is in deployment. It is suggested that the Firewall should have atleast 2 x 10G interfaces for DMZ & MZ connectivity		No changes required, 1 G ports will suffice the connectivity of DMZ ports. Bid will be evaluated as per tender specifications.	

43	Fortinet	Firewall and NIDS	32	2.3 Technical specification for Firewall and NIDS Solution - Point No -1.8	Firewall should support 1 Million concurrent firewall sessions	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. To cater to such high sessions requirement it is suggested that the Firewall should cater to at least 10 Milion concurrent sessions		No changes required, capacity planning has already been done based on the servers and no. of consumers. Based on the inputs and requirement, firewall should support 1 million concurrent firewall sessions.
44	Fortinet	Firewall and NIDS	32	2.3 Technical specification for Firewall and NIDS Solution - Point No -1.11	It should have 1TB of Total Hard Drive Capacity	Request to please provide option of External appliance for logging & reporting as having internal 1TB storage is hardly available with any Firewall OEMs		It should have 500 GB of total hard drive capacity (internal or external)
45	Fortinet	Firewall and NIDS	33	2.3 Technical specification for Firewall and NIDS Solution - Point No -2.4	Should have in-built redundancy for storage, if applicable and power	Request to please remove storage redundancy as Firewalls / IPS do not have internal storage options in redundancy mode		system needs to have in built redundancy, bid will be evaluated as per tender specifications.
46	Fortinet	Firewall and NIDS	34	2.3 Technical specification for Firewall and NIDS Solution - Point No -7.2	Fails open should a Power loss/Ethernet/hardware/software failure occur	Since IPS is part of Firewall , it will be deployed in NAT mode so request to please remove fail open option		IPS will be independently deployed without integration of firewall. Fail open feature is required in case one or both the IPS is not available.
47	Fortinet	Firewall and NIDS	37	2.3 Technical specification for Firewall and NIDS Solution - Point No -14.4	Can export reports to other formats. Users should be able to output report data into a variety of different file formats like HTML, PDF, CSV, and Printer	Request you please remove CSV, and Printer as mostly OEMs support HTML & PDF		CSV format is a requirement for NIDS reporting, same cannot be removed. Bid will be evaluated as per tender specifications.
48	Pace				Section 2.2 System Security Solution seems to have been taken from R-APDRP specifications where the scope of vendor was comprehensive and spanned across all business applications, hardware, networking and data center implementation. Therefore, in that tender and scope of work, these requirements were relevant. In this tender the scope of work is very limited and these security requirements cannot be complied alone by the respondent of this tender. It will require services and active participation from vendors of all main business applications, networking and data center. We request you to review these requirements and limit their scope to the software and hardware being implemented via this tender only. A complete rewording/ re-scoping of this section is requested in view of this issue.			System security solution is excluded from the tender, Please refer amendment.

49	Pace				The audit requirements are already covered for each individual specs. They need not come in Section 2.2. E.g. In Identity Management specs, points in 7.x are related to audit and security implementation specific to Identity Management solution.			Bid will be evaluated as per technical specifications mentioned in tender.
50	Pace				Ss1.6 – DR scope should also be limited to the software and hardware defined in the scope of this tender. The respondent of this tender cannot own entire DR responsibility.			Bidder needs to implement software and hardware at DR as per defined terms in tender.
51	Pace				Similarly all other points mentioned in 2.2 for encryption, versioning, secure data transfer, scope control, change control, web service security, documentation should also be limited to the software and hardware supplied via this tender and should be reworded.			Bid will be evaluated as per technical specifications mentioned in tender.
52	Pace				Please define the integration requirements clearly. Who will be responsible for integration Identity Management etc with existing software? If the respondent is responsible, please provide list and details of the softwares for which Identity management, Single-Sign-on etc. have to be integrated.			Successful bidder will be responsible for integration of all the available software at Data Centre. common software available will be SAP modules, GIS, exchange, AD and other home grown applications.
53	Pace				Who will be responsible for operations of these tools once they are implemented? E.g administrative activities and operational day-to-day activities such as access provisioning, user creation. The tender only mentions about support of 5 years.			Successful bidder will be responsble for any issue in operation and maintenance job as per terms and conditions of tender
54	Pace				Will you provide remote access to data center for our teams to work on the project?			Providing remote access for implementation is not possible.