आरईसी पावर डिस्ट्रीब्यूशन कम्पनी लिमिटेड
REC POWER DISTRIBUTION COMPANY LIMITED
(A wholly owned subsidiary of REC Ltd., a 'Navratna CPSE' under Ministry of Power. Govt. of India)
CIN no. of RECPDCL- **U40101DL2007GOI165779**
POWER DISTRIBUTION
ISO 9001 : 2008 Certified Company
ISO 14001:2004 Certified Company
Corporate Office: 1016-1023, 10th Floor, Devika Tower, Nehru Place, New Delhi-110019
Tel: 011-4412 8755 Fax: 011-4412 8768, Web: www.recpdcl.in, E-mail: recpdcl@rediffmail.com
Regd. Office: Core-4, SCOPE Complex, 7 Lodhi Road, New Delhi-110003, Phone (011) 43091506 Fax: (011) 24365815

Notice Inviting Tender

(Tender invited through e-Tendering mode only)

For

Rate Contract of Supply and installation of IT Security Solution (Hardware and Software)

No. RECPDCL/TECH/IT Security-GED/e-Tender/2015-16/1518 Dated:04.09.2015

Description of task, Pre-qualifying criteria, e-tender submission format and procedure is available on REC Power Distribution Company Limited (RECPDCL) website (www.recpdcl.in), Rural Electrification Corporation (REC) website (www.recindia.nic.in), Central Publication Portal (www.eprocure.gov.in)

Important Dates for E- Tendering mode	
Date of Release of NIT	**04.09.2015**
Last date for queries / seeking clarification	**09.09.2015 at 1800 Hours**
Pre Bid Meeting	**10.09.2015 at 1030 Hours**
Last date of submission of Tender	**21.09.2015 at 1500 Hours**
Date of Opening of Technical bid	**21.09.2015 at 1600 Hours**
Date of Opening of Financial bid	**To be intimated later**

Note:

Online registration shall be done on e-tendering website i.e. www.tenderwizard.com/REC & in general, activation of registration may takes 24 hours subject to the submission of all requisite documents required in the process.

-Sd-

(S.C. Garg)

Addl. C.E. O.

[This document is meant for the exclusive purpose of Agencies participating against this bid and shall not be transferred, reproduced or otherwise used for purposes other than that for which it is specifically issued]

INDEX

SECTION-I

TENDER INFORMATION

Name of the assignment: Purchase of IT Security Solution (H/w and S/w)

Si. No.	Event	Information to the agencies
1	Date of Release of NIT	**04.09.2015**
2	Last date for queries / seeking clarification	**09.09.2015 at 1800 Hours**
3	Pre Bid Meeting	**10.09.2015 at 1030 Hours**
4	Last date of submission of Tender	**21.09.2015 at 1500 Hours**
5	Date of Opening of Technical bid	**21.09.2015 at 1600 Hours**
6	Date of Opening of Financial bid	**To be intimated later**
7	Pre- Bid Meeting Address	REC Power Distribution Company Limited, 1016-1023, 10th Floor, Devika Tower, Nehru Place, New Delhi- 110019, India Fax : 011-4128768
8	Tender Document	The details can be downloaded free of cost from the websites www.recpdcl.in (or) www.recindia.nic.in (or) www.eprocure.gov.in (or) www.tenderwizard.com/REC
9	EMD #	Rs.2,50,000/-
10	Address for Bid submission	**Shri Subhash Chandra Garg,** Addl. Chief Executive Officer, REC Power Distribution Company Limited, 1016-1023, 10th Floor, Devika Tower, Nehru Place New Delhi- 110019, India. Fax : 011-4128768 Email- recpdcl.goa@gmail.com/recpdcl@rediffmail.com
11	Contact Person	**Shri Sunil Bisht ,** Assistant Manager (Technical) REC Power Distribution Company Limited (RECPDCL) Phone:011-44128760; Fax:011-44128768 Email- recpdcl.goa@gmail.com/recpdcl@rediffmail.com

 # The EMD (Earnest Money Deposit) is to be submitted by all the participating Bidders in the form of demand draft/Bank Guarantee of an amount of Rs.2,50,000/- (Two Lakhs and Fifty Thousand only/-.) of any schedule Indian bank in favour of REC Power Distribution Company Limited, Payable at New Delhi .The EMD of unsuccessful Bidder will be returned within 180 days from the period of expiry of NIT and EMD of successful Bidder will also be returned after acceptance of work order and submission of PBG (Performance Bank Guaranty) i.e. 10% of the Contract Value (within 30 days from receipt of PBG).

The bid shall remain valid for a period of 180 days from the date of bid submission.

SECTION-II

PREFACE

Goa Electricity Department (GED) has recently awarded IT Implementation Works under Part-A of R-APDRP Scheme to M/s REC Power Distribution Company Limited (RECPDCL) with Tata Power Delhi Distribution Limited as its Technology Partner.

The Scope of Services includes Preparation of Base-line Data System for the project area covering Consumer Indexing, GIS Mapping, Automatic Metering (AMR) on Distribution Transformers and Feeders, and Automatic Data Logging for all Distribution Transformers & Feeders and SCADA / DMS system for big cities only. It would include Asset Mapping of the entire distribution network at and below the 11kV transformers and include the Distribution Transformers and Feeders, Low Tension lines, poles and other distribution network equipment. It will also include adoption of IT applications for meter reading, billing & collection; energy accounting & auditing; MIS; redressal of consumer grievances and establishment of IT enabled consumer service centers etc.

In addition to the Towns and Cities with a population of more than 30,000 (10,000 in case of Special Category States) as per population data of 2001 Census in Goa, the certain high-load density rural areas with significant loads, works of separation of agricultural feeders from domestic and industrial ones, and of High Voltage Distribution System (11kV) will also be taken up in R-APDPRP Part-A scheme and accordingly four towns have been identified to be covered under the scheme as per the details mentioned in Table 1.

Goa, a tiny emerald land on the west coast of India, the 25th State in the Union of States of India, was liberated from Portuguese rule in 1961. It was part of Union territory of Goa, Daman & Diu till 30 May 1987 when it was carved out to form a separate State. Goa is India's smallest state in terms of area and the fourth smallest in terms of population. Located on the west coast of India in the region known as the Konkan, it is bounded by the state of Maharashtra to the north and by Karnataka to the east and south, while the Arabian Sea forms its western coast.

Panaji (also referred to as Panjim) is the state's capital. Vasco da Gama is the largest city. The historic city of Margao still exhibits the influence of Portuguese culture and renowned for its beaches, places of worship and world heritage architecture, Goa is visited by hundreds of thousands of international and domestic tourists each year. It also has rich flora and fauna, owing to its location on the Western Ghats range, which is classified as a biodiversity hotspot.

Goa covers an area of 3702 square kilometers and comprises two Revenue district viz North Goa and South Goa. Boundaries of Goa State are defined in the North Terekhol River which separates it from Maharashtra, in the East and South by Karnataka State and West by Arabian Sea. Goa lies in Western Coast of India and is 594 Kms (by road) away from Mumbai city.

Goa, for the purpose of revenue administration is divided into district viz. North and South Goa with headquarters at Panaji and Margao respectively. The entire State comprises 11 talukas. For the purpose of implementation of development programmes the State is divided into 12 community development blocks. As per 2001 census, the population of the State is 13,42,998. A very striking feature of Goa is the harmonious relationship among various religious communities, who have lived together peacefully for generations. Though a late entrant to the planning process, Goa has emerged as one of the most developed States in India and even achieved the ranking of one of the best states in India with regards to investment environment and infrastructure.

This NIT is being floated to procure IT security solution (H/w and S/w) to be deployed in data center and DR site of Goa electricity department. IT security solution comprises primarily of the enterprise firewall with IPS & IDS support, mail filtering, content filtering, anti-virus for desktop and laptops and reverse proxy.

The Basis Statistics of GED				
Name of Town	**Area in Sqkm**	**Network Length**	**No. of Consumers**	**No. of Transformers**
Panjim	506	14220	5.16 Lacs	5000
Margao	1391			
Mapusa	1239			
Marmagao	109			

Above data is only for reference and may vary in actual

Information of Project Areas				
Name of Project Area (town)	**Number of Subdivisions Offices**	**Number of Other Offices**	**Nearest Railway Station to HQ**	**Nearest Functional Airport to HQ**
Panaji	8	25	Carambolim	Dabolim Airport
Marmagoa	4	19	Vasco Da Gama	Dabolim Airport
Margoa	10	62	Madgao	Dabolim Airport
Mapusa	8	85	Tivim	Dabolim Airport

SECTION-III

Instructions to Bidders

3.1 Submission of Bid

Bidders shall submit their responses online through e-tendering website www.tenderwizard.com/REC

A. The submission and opening of Bids will be through e-tendering process.

Bidder can download Bid document from the RECPDCL web site i.e. http://www.recpdcl.in or www.recindia.nic.in or www.eprocure.gov.in and RECPDCL's e-tendering portal i.e. www.tenderwizard.com/REC

***(Note:** To participate in the e-Bid submission, it is mandatory for agency to have user ID & Password. For this purpose, the agency has to register them self with REC PDCL through tender Wizard Website given below. Please also note that the agency has to obtain digital signature token of class-III for applying in the Bid. In this connection vendor may also obtain the same from tender Wizard.)*

Steps for Registration

(i) Go to website http://www.tenderwizard.com/REC
(ii) Click the link 'Register Me'
(iii) Enter the details about the E-tendering as per format
(iv) Click 'Create Profile'
(v) E-tender will get confirmation with Login ID and Password

Note- Online registration shall be done on e-tendering website i.e. www.tenderwizard.com/REC & in general, activation of registration may takes 24 hours subject to the submission of all requisite documents required in the process. It is sole responsibility of the bidder to register in advance.

B. Steps for application for Digital Signature from Bid Wizard:

Download the Application Form from the website http://www.tenderwizard.com/REC free of cost. Follow the instructions as provided therein. In case of any assistance you may contact RECPDCL officers whose address is given at the Bid.

Bid to be submitted through online mode on website www.tenderwizard.com/REC in the prescribed form.

C. The Agency qualifying the criteria mention in section VI should upload Bid document with duly signed scanned soft copy of the documents given below for the prequalifying response:

Pre- Qualifying Criterion Documents/Technical Bid

1 Form-I ----------Letter of submission of Tender
2 Form-II ----------Pre-Qualifying Criteria Details
3 Form-IV ----------– No Deviation Certificate
4 Form-V ----------Manufacturer Authorization Form
5 Annexure-B ------Acceptance form for participation in reverse auction event

EMD of Rs. 2,50,000/- in form of DD or Bank Guarantee may be drawn from a scheduled commercial bank in favour of The “REC Power Distribution Company Ltd”, New Delhi and scanned copy to be uploaded and original to be submitted before the last date & time of Submission of Tender.

Financial Bid

1. Form-III---------Financial Proposal (to be submitted through online mode only)

Financial bid to be submitted in the specific format designed same may be downloaded from website www.tenderwizard.com/REC and after filling the form it is to be uploaded through digital signature.

The all document should be addressed to.

Addl. Chief Executive Officer REC Power Distribution Company Ltd. 1016-1023, 10th Floor, Devika Tower, Nehru Place, New Delhi - 110019

(Note:** All papers that comprise the Bid document of the concerned Bid must be numbered. An index of each page should also be provided**)

SECTION-IV

SCOPE OF WORK & SERVICE LEVEL AGREEMENT

1. Detailed Scope of Work

1. The scope covers supply, installation and commissioning of IT security hardware / software at DC and DR site.
2. The Bidder shall also be responsible for manufacture, inspection at manufacturer's works, supply, transportation, insurance, delivery at site, unloading, storage, complete supervision, successful installation, commissioning and user acceptance of all hardware and software related to IT security at DC and DR site.
3. Any item though not specifically mentioned, but is required to complete the project works in all respects for its safe, reliable, efficient and trouble free operation shall also be taken to be included and the same shall be supplied and installed by the Bidder without any extra cost.
4. The bidder's proposal shall include the list of special tools, testing equipment and accessories required for day to day operation and maintenance of the system. All such tools shall be supplied by the bidder. The bidder should clearly bring out the list of such tools along with itemized price in the bid. However the prices of these special tools shall be included in the lump sum bid price and would be considered for the bid evaluation.
5. The bidder shall design and provide the hardware at DC & DR site with suitable expandability for covering the entire utility area at a later date along with a 7.5% per annum growth in consumer and asset base for next five years.
6. The supply of all required cables, power cords, rack mountable kits etc. to be provided as per Indian standards.
7. Supply, installation and commissioning of Operating Systems and associated software, tools etc. as applicable in all equipment is in the scope of bidder. Bidder shall supply two copies of media of all related software.
8. All supplied items must conform to the detailed technical specifications mentioned in this tender document.
9. Packaging and transportation from the manufacturer's work to the site including port and customs clearance will be borne by the bidder.
10. Receipt, storage, preservation and conservation of equipment at site is in the scope of bidder.
11. Insurance of all equipment from manufacturer's site till installation, commissioning, handing over and user acceptance will be borne by the bidder.
12. Bidder shall maintain the mandatory and recommended spares during warranty and AMC period and provide the list of the same.
13. Bidder shall install the equipment, obtain user acceptance and submit a copy of user acceptance to designated authority.
14. Whenever a material or article is specified or described by the name of a particular brand, manufacturer or trade mark, the specific item shall be understood as establishing type, function and quality desired. Products of other manufacturers may also be considered, provided sufficient information with necessary certificates and documents are furnished so as to enable the RECPDCL to determine that the products are equivalent to those named. The Decision of RECPDCL shall be final and binding on the bidder in this regard. In case bidder proposes the products of other manufacturer, necessary certificates and documents shall be submitted along with the bid.
15. The bidder shall provide 3 years onsite warranty and 2 years Annual Maintenance Contract (AMC) of all supplied, installed and commissioned equipment as per Service Level Agreement (SLA).

16. The Bidder shall be responsible for providing all material, equipment and services specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability and the reliability of the complete work covered under this specification.
17. It is not the intent to specify all aspects of design and installation of associated systems mentioned herein. The systems, sub-systems and equipment/devices shall conform in all respect to high standards of engineering, design and workmanship, and shall be capable of performing continuous commercial operation.
18. **Arrangement by bidder**

    The bidder shall make his own necessary arrangements for the following and for those not listed anywhere else:

    - Office and store.
    - Transportation.
    - Boarding & lodging arrangement for their personnel

    The bidder shall also provide all the construction equipment, tools, tackles and testing kits/equipment required for pre-assembly, erection/installation, testing and commissioning of the equipment and system covered under the Contract. He shall submit a list of all such materials to the Engineer before the commencement of work at Site. These tools and tackles shall not be removed from the Site without the written permission of the Engineer-in-charge.
19. **Training**

    Training of employees is in the scope of bidder. Standard curriculum, designed and agreed by the owner for hardware, software etc. preferably from the OEM partner or OEM's certified training partner shall be arranged. The bidder is required to quote on per person basis for this training. The Purchaser will prefer if a portion of the training is conducted on-site.
20. **Documentation**

    The bidder will provide ongoing product information for referential purposes and facilitating self-education by Utility personnel. The following documents (one set each) will be required for smooth functioning of the system at DC and DR site. Following documentation is included in the standard license fee, for example:

    - User manuals
    - System administrator manuals
    - Technical manuals
    - Installation guides
    - Business process guides
    - Program flow descriptions
    - Data model descriptions
    - Sample reports
    - Screen formats
    - Toolkit guides
    - Troubleshooting guides
    - Frequently asked question (FAQ) guides

21. Bidder has to indicate the space requirement and heat load for various equipment at DC and DR site, any other specific requirement, power supply requirement including standby supply requirement etc.

22. **Software tools**

    Software tools must be latest versions that are currently supported by manufacturer, if relevant. Software tools must be compliant with generally accepted standards and accommodate Utility's plan for the future expansion of systems. Utility also expects tools and automation to feature in the implementation so as to maximize the efficiency and quality of the implementation project.

23. Spares

a) The Bidder shall include in his scope of supply all mandatory and commissioning spares related to Hardware requirements. The bidder has to quote for the mandatory spares requirement for 5 years operation after warranty period. List of such spares along with the quantities shall be indicated in the bid and shall be considered for bid evaluation purpose.
b) All spares supplied under this contract shall be strictly interchangeable with the parts for which they are intended for replacement. The spares shall be treated and packed for long-term storage in the climatic conditions prevailing at the project site. Small items shall be packed in sealed transparent plastic covers with desiccant bags as necessary.
c) The bidders shall attach the storage conditions requesting covered storage or storage under air conditioned environment as appropriate for certain classes of spares.
d) Each spare part shall be clearly marked and labelled on the outside of the packing together with the description when more than one spare part is packed in single case. A general description of the contents shall be shown on outside of the case and detailed list enclosed. All cases, containers and other packages must be suitably marked and numbered for the purpose of identification.

24. Commissioning Spares

The Bidder shall supply spares, which he expects to consume during installation, testing and commissioning of the system. The quantity of these spares shall be decided based on his previous experience, such that site works shall not be hampered due to non-availability of these spares. Bidder shall submit a complete list of such spares along with the bid, the cost of which shall be deemed to have been included in the lump sum proposal price of the package. The unused commissioning spares may be left at the site for use by the Owner, if so agreed at a cost to be negotiated. No spares except commissioning spares will be used during the commissioning of the system before take over by the Owner. In case of extreme urgency, if spares other than commissioning spares are used by bidder for commissioning of the system, the same will be required to be recouped free of charges.

25. Quality Assurance Plan

The bidder shall have a comprehensive quality assurance program at all stages of manufacture/ development/ implementation for ensuring products giving reliable, trouble free performance. The bidders shall furnish the details of their quality assurance plan and test set up along with the bid. A detailed quality assurance program shall be finalized with the successful bidder during the award stage. However, the Quality Assurance Plan shall conform to the following standards–

IS/ISO/IEC 27001 – ISMS
IT Security, IT services (10 Standards) - All harmonized with ISO/IEC
LITD 16 – Standards on Computer Hardware
IS 13252:2003/IEC 60950

26. The bidder shall adhere to all the terms mentioned in the service level agreement (SLA).

27. Additional Scope for DR site

1. The Supply of equipment, software etc. for DR site should commence only after completion of 80% work of the package and DR site shall be commissioned only after successful go live of at least 70% Town as per the scope of work.
2. The Bidder's scope of work as per the conditions of contract and technical specifications includes assembly, quality check, packing, supply, transportation, transit insurance, local delivery, receipt, unloading, handling, storage at site, movement at DR site,
   conduiting, cabling, installation, testing and commissioning of IT security hardware / software at DR site with its associated peripherals and also include documentation, warranty, and training of Owner's personnel for the said System.
3. The Bidder's responsibility shall specifically include the following
   a. The complete System including all the hardware, Software and caballing equivalent to the items supplied at primary Datacentre and/ or as agreed upon mutually with owner to be supplied at DR centre and the same must operate at or above the guaranteed values with regard to availability.
   b. Any software updates, upgrades released till the completion of warranty and FMS (Facility Management Services) period shall be supplied free of cost and installed and commissioned free of cost as per instructions from owner.
   c. The Bidder shall post his Service Engineers at Owner's Site till the completion of Acceptance test.
4. The scope of installation and commissioning shall include the following –

   i. The bidder in consultation with OWNER site engineer shall determine the exact positioning of equipment's, Installation, housing of equipment and cable routing. The bidder shall prepare his proposed plan and estimate the quantities for support material required, racks, extension boards, power requirement, cables, conduit/ channels as desired within specified limit of the contract.
   ii. The Bidder shall be fully responsible for installation and commissioning of the IT security hardware / software and other related activities for erection, testing and commissioning.
   iii. All power and connecting cables, conduits/channel laying shall be as per approved routing by OWNER. Installation of all hardware and software as approved by OWNER, along with Distribution of electrical power to various equipment's.
   iv. Installation of equipment's, software as required.
   v. Field testing and commissioning of system.
   vi. Installation, configuration, and testing of the system in consultation with the Owner. Preparation of the system to make it ready for installation of Application packages as applicable.
   vii. Commissioning of Disaster Recovery System shall be as per technical specification.

28. Availability Test

(a) After successful completion of installation and configuration availability test shall be conducted for minimum 10 days continuously. The percentage availability shall be defined as:

$$\frac{\text{(Test Duration Time - System Outage Time)} \times 100}{\text{(Test duration Time)}}$$

The test duration time shall be exclusive of external power failure time.

(b) The system shall be considered as “available”, if all the equipment’s connected are up and running in unavailability of raw power.
(c) The availability shall be worked out daily and shall be checked on a cumulative basis. Thus, if the available time on 2 consecutive days is x and y hours respectively and test duration time is a and b hours respectively, then the availability to be reckoned at the end of 2 days is 100 (x + y) / (a + b). During the 30 days of continuous testing, if this cumulative availability is less than 98% then the contracted Bidder shall do the necessary rectification and/or replacement of system/sub-systems as deemed fit by him at his risk and cost. The availability of 98% shall again be demonstrated by the Bidder over a period of 10 days after the Bidder has performed necessary rectification and/or replacements.
(d) However, if the system does not meet the availability criteria laid down as above within 90 days after installation & commissioning, the System shall be required to be replaced by a new system. The bidder shall replace the system or sub-system within 6 weeks of the direction to that effect from the owner. However the rejected system shall be allowed to be removed only on receipt of replacement system.

29. Acceptance

System shall be accepted by the owner after successful completion of Availability test and establishment of complete setup as per scope of work.

2. Technical Specifications

(i) The supplier shall submit the data sheets for each of the equipment model /software detailing the specifications of the equipment.
(ii) The equipment models shall be supported by the OEM for a minimum period of next 5 years.

2.1. Technical specification for Identity and Access Management System

S.no	Feature	Functionality	Bidder Response (Compliant / non-compliant)
1	**Adapter/ connector Support**		
1.1	Solution Compatible	The proposed solution should be compatible on all the operating systems offered by the bidder in the proposed solution including client machines which are most likely window based system.	
1.2	Out of box workflow	Identity management for user provisioning should have out of the box workflow for automating approvals for user access management, self-registration and self-care functionality for reducing the administrative load and manual intervention.	
1.3	IDE to design Work - Flow	The solution should provide an IDE to design the workflows.	
1.4	Standard for Workflow implementation	The proposed solution should support "Workflow Management Consortium (WfMC) TC-1003 Workflow Reference Model standard for workflow implementation".	
1.5	Connector availability for target systems	Identity Management Solution should have Connector availability for all target systems that need to be managed.	
1.6	Connector development tool	The proposed solution Should provide resource kit or an SDK to add new Resource adapters.	
1.7	Agent-less Architecture	Identity Management solution should be Agent-less Architecture and use gateways where agent is required.	

1.8	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	
1.9	Indexing	The solution should leverage an intelligent indexing system to manage user identities and access privileges, leaving account information with the information owner and thus avoiding the time-consuming effort of building and maintaining another user repository.	
1.10	Discovery and Correlation of user Account	The Proposed solution should provide an automated way to discover and correlate all accounts associated with an individual to speed the account mapping process.	
1.11	User Repository	The solution should use separate repository for user data and audit log information.	
1.12	Open Provisioning Standard	The solution should support open provisioning standard like SPML.	
1.13	Authentication/authorization framework	The solution should allow enterprise applications and platforms to integrate into the centralized authentication/ authorization framework seamlessly. The solution should support both thick client as well as web based applications.	
1.14	Access Management	The Access Management solution should be capable of running on web servers as well as application servers.	
1.15	Pluggable authentication module	The proposed solution should provide the ability for pluggable authentication module, and new auth modules should be able to be added via an SDK.	
2	**Access Rights Capabilities and Access Control**		

2.1	Data protection	Sensitive customers' data must be protected in accordance with guidelines that will be agreed with the Purchaser.	
2.2	Entry screens	On completion of successful logon, the following information shall be displayed : a) Date and time of previous successful logon. b) Details of any unsuccessful logon attempts since the previous successful logon. Reminder of the onus of the user to bring to notice any aberration observed.	
2.3	Unsuccessful logon attempts	After predefined number of consecutive unsuccessful attempts to logon to a user Id, that user id shall be disabled against further use until the same is enabled by System Administrator	
2.4	Application time out	Terminal / User Id time-out shall occur if a terminal / user ID remains logged onto a system/ application but remains inactive for a predefined time. If the terminal is dedicated to one application then timeout shall occur after a predefined time inactivity. The screen shall be cleared of any information when time out occurs.	
2.5	Limited application software on key systems	Software which can be used to modify existing programs on systems / applications, e.g. editors and compilers, shall have access restricted to authorized staff only. Any such software which is not needed for operational reasons shall be removed after the modifications have been made.	
2.6	Segregation of duties	Clear segregation of duties between user groups is necessary to minimize the risk of negligent or deliberate system misuse. In particular segregation must be implemented between: 1. Business use. 2. Computer operations. 3. Network management. 4. System administration. 5. System development & maintenance. 6. Change management. 7. Security administration. 8. Security audit. Where it is operationally not possible to adhere to this policy advice shall be sought from the Purchaser on security. As a minimum, the above segregation shall be enforced at the User Id level i.e. the above functions shall not be allowed from the	

		same User Id.	
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.	
2.8	Controlling User's access	The system shall provide a mechanism to authorize users to access the system, revoke users from accessing the system, and modify the security information associated with users. The system shall also be able to automatically suspend or roll back a reconfigured account that violates policy.	
2.9	Restricted access to resources	The system / resources shall provide a mechanism to allow or deny specified user IDs to access the system during specified ranges of time based on time-of-day, day-of week, and calendar date.	
2.10	Console operations for privileged users	The system shall provide a mechanism to allow or deny specified user IDs to access the system based on means of access or port of entry.	
2.11	Resource, access control list	For each resource, the system shall provide a mechanism to specify a list of user IDs or groups with their specific access rights to that resource (i.e. an access control list). Solution shall provide for grouping of users and assigning ACL to the group.	
2.12	Group ACL vs individual ACL	Group ACL should be aggregated to individual user's ACL and in case of conflict, user's ACL shall govern.	
2.13	Grant and deny access	System shall provide both Grant and Deny to a resource.	

2.14	Individual access rights to users	The system shall have ability to assign users individual access rights and to define access rights available to users in a role upon their request and approval.	
2.15	Job based access to information	The system shall have ability for different personnel to view different levels of information based on their job duties.	
2.16	Modifications to the access list	The system shall provide a mechanism to modify the contents of a resource's access control list.	
2.17	Change in Access rights	The System shall have ability to associate access-rights definition with a role within the organization and dynamically and automatically change access rights based on changes in user roles. The system shall also have ability to set designated times for changes in access rights or policies.	
2.18	Rules for routing approvals	System should also use defined rules/ information specific to utility to determine routing of approvals.	
2.19	Access rights change notification	The system shall be able to compare local administrator changes against a system-of-record of account states to determine if changes comply with approved authorities and policies and shall be able to notify designated personnel of access rights changes made outside the provisioning solution, if any.	
2.20	Audits on user accounts	The solution should provide the capability to do half yearly audits on the lines of ISO 17799/BS7799 for user accounts.	
2.21	Resource ownership	The system shall provide a mechanism to identify all resources in the system that are owned by a specified user ID, the resources to which that user ID is allowed access and the specific access rights for each resource.	
2.22	User's authority changes	System shall also be able to detect, evaluate and respond to user authority changes made directly to a resource.	
2.23	Restrictive access	Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource.	
2.24	Restricted access to access control information	The system shall protect all information used for resource access control decisions (e.g., access control lists, groups lists, system date and time)	

2.25	Policy simulation	The system shall provide policy simulation and 'what-if' modeling of changes, i.e. simulation of effects of policy changes before they are enacted, reporting errors, or potential problems, and ability to resolve before live operations.	
2.26	Monitoring of access controls	The system shall monitor the followings :- • Successful logins and login attempts e.g. Wrong user ID/Password, and login patterns • Rejected access attempts because of insufficient authority • All usage by privilege users e.g. Powerful access to system utilities or applications • Use of sensitive resources e.g. Access to highly sensitive data • Change to access rights of resources • Changes to the system security configuration • Modification of the package software • Changes to user privileges.	
2.27	Reporting on user roles and rights	The system shall have ability to report on roles, rights associated with roles and users associated with roles.	
2.28	Flexible connection to multiple data stores	The system shall have flexible mechanisms to connect to multiple data stores containing accurate information on valid users.	
2.29	Identity store information in real time	The system shall have ability to load identity store information on a scheduled bulk basis and to detect and respond to identity store changes in near real time.	
2.30	Retrieval of account information	The system shall have ability to retrieve account information from target managed resources on a scheduled basis, both in bulk or in filtered subsets to preserve network bandwidth	
2.31	Real-time local administrator account maintenance	The system shall have ability to detect and report in near real-time local administrator account maintenance (creation, deletion, changes) made directly on local resources natively.	
2.32	Support for prerequisite services	The system shall define services that must be granted prior to creation of the access rights. For example, Microsoft ® Windows NT ® rights must be granted prior to granting rights to Exchange Support for entitlement defaults and constraints (each characteristic of an entitlement may be set to a default value, or its range can be constrained, depending on the capabilities of the entitlement to be granted)	

3	**User Administration**		
3.1	Creation of standard User Profile	A mechanism must exist to allow a range of User Ids to be built with a standard user profiles of multiple categories, e.g. Data entry user, data modify user at the section office, division office etc.	
3.2	Dormant User	Where a user Id remains unused for a pre-specified number of consecutive days, it shall be disabled. If no authorized request for reinstatement is received within a further predefined time period, the user Id shall be deleted. The user would be informed before this happens.	
3.3	Segregating user access to system	All user Ids shall be set up with privileges that limit the use of the user Id to designated areas only and to ensure that other functions cannot be performed by the user ID for which they are not authorized. Some user IDs have powerful privileges associated with them and these shall only be provided and maintained by the system administrator. To prevent the provision of user IDs with privileges associated to them, when these are not required by the user, any templates used to set up user IDs shall have no default privileges associated with them.	
3.4	Unique User ID	System shall be able to create unique user IDs using a set of consistent algorithms and defined policies of the owner and not in current use or previous use by the organization and not shared with others. The system shall provide a mechanism to associate specified information (e.g., user name and affiliation) with each user ID.	
3.5	ID conventions	Procedures for user account management should define the naming convention for user IDs and the operations practices for provisioning and removing these user Ids.	
3.6	Differentiating normal and privileged users	User Ids shall not consist of less than a predefined number of characters. The number of characters would be different for normal users and privileged users;	
3.7	Single account with multiple authorities	The system shall have ability to create a single account with multiple authorities governed by different policies.	

3.8	Temporarily Disabling	The system shall provide a mechanism to administratively disable user IDs and a mechanism for re-enabling or deleting a disabled user ID after a specified period of time. The use of this mechanism shall be privileged.	
3.9	Active Users	The system shall internally maintain the identity of all active users.	
3.10	Tracking User IDs	The system shall provide a mechanism to obtain the status of any user ID.	
3.11	Grouping User IDs	The system shall provide a mechanism that allows a collection of user IDs to be referenced together as a group.	
3.12	Limiting multiple log on	For those systems that have the architecture to support multiple logons per user ID, the system shall provide a mechanism that limits the number of multiple logon sessions for the same user ID. The mechanism shall allow limits for user IDs and groups to be specified. The system default shall limit each user ID to one simultaneous logon session. As per business process requirement, particular machine ID's to permit login by selected users only.	
3.13	Associating IDs to processes	The system shall provide a mechanism by which the user ID associated with a process can change to a user ID that would provide any additional privileges.	
3.14	Assignment of one or more roles to users	The system shall be able to assign users to one or more roles and can implicitly define subsets of access to be unavailable to a role.	
4	**Self-Regulation User Administration capabilities**		
4.1	Adherence to open standards	The system shall adhere to open standards.	
4.2	Secure environment	The system shall have secure environment for transmitting access changes across the Internet.	
4.3	Protection of private user information	Protection of private user information through secure facilities and sound processes.	
4.4	Reporting of user rights	Reports of user rights into external systems, sponsors of users and audit trails of access rights changes.	
5	**Authentication**		
5.1	Authentication	The system shall provide a mechanism to	

	mechanism	authenticate the claimed identity of a user.	
5.2	Single authentication procedure	The system shall perform the entire user authentication procedure even if the user ID that was entered was not valid. Error feedback shall contain no information regarding which part of the authentication information is incorrect	
5.3	Modification Ability to authentication information	The system shall provide a mechanism to support the initial entry or modification of authentication information.	
5.4	Privileged access to authentication data	The system shall require a privilege to access any internal storage of authentication data	
5.5	2-Factor authentication	System should support two factor authentication (Biometrics, tokens etc.)	
6	**Password Management**		
6.1	Password confidentiality	System shall be able to securely deliver User Ids and passwords to new users electronically. User Ids and passwords, when conveyed electronically shall only be visible to the person for whom they are intended e.g. after the user has logged on to the appropriate electronic system.	
6.2	Password protection	All electronic information systems and applications shall have a password management system which meets the following requirements : a) Enforces change of initial password at first logon. b) Allows users to select and change their own passwords at any time subsequently. c) Have ability to implement password formation rules to enforce password strength across the organization, e.g. minimum character length of password, password as a combination of numeric, alphabets & special characters d) Have validation routines built in which, as far as possible, check that the password selected is a quality password as defined in a Policy Document to be handed over to the Purchaser at the time of implementation. e) have a confirmation process on changing passwords to cater for typing errors	

		f) have ability to deliver password-change success failure status to requestor electronically g) have the ability to enforce password change after every n days. If the password is not changed in the pre specified number of logins then the ID should be disabled requiring re-enabling by System Administrator. h) Prevents reuse of passwords within a specified period/number of times. i) Does not echo passwords to screen or paper. j) Stores passwords in a one-way encrypted form away from the system/ application data files in a protected password file that is access controlled such that no users can read or copy the encrypted contents. k) Prohibit use of null passwords l) Have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user m) Have a challenge-response system to authenticate a user with a forgotten password by using shared secrets.	
6.3	Unique passwords	The system shall provide no mechanism whereby multiple user IDs explicitly shares a single stored password entry. The system shall provide no means to facilitate the sharing of passwords by multiple users.	
6.4	Clearing passwords	The system shall allow a user to choose a password that is already associated with another user ID. The system shall provide no indication that a password is already associated with another user ID.	
7	**Audit Trails & Reports**		
7.1	Time-stamped records	The system must maintain- • Time-stamped records of every access change request, approval/denial, justification and change to a managed resource • Time-stamped record of every administrative and policy-driven change to access rights	

7.2	Audit Trail reporting	The system must provide reports on audit trails for users, systems, administrators and time periods, including workflow approvals, rejections, request statistics, policy compliance and Audit reports, User account reports, Access reports and Service reports and also any customized reports based on specific need.	
7.3	Maintaining audit trails	Audit trail records shall be retained in a tamper proof environment in accordance with the Purchaser's policy for a reasonable amount of time to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.	
8	**Distributed Administration**		
8.1	Defining of organizational structures	Ability to define organizational structures based on the access granting authority	
8.2	Delegation of administrative tasks	Ability to delegate each administrative task with fine-grained control at Organizational Unit Level so that the team or Dept. Admins can completely perform the Administrative tasks for their Organization Unit.	
8.3	Access to delegated capabilities over web	Ability to access all delegated capabilities over the Web via Web Browser with a zero-footprint client.	
8.4	Web access control with single sign-on environment	Ability to incorporate Web access control with single sign-on environment and to distribute provisioning components securely over WAN and Internet environments, including crossing firewalls.	
8.5	Enterprise Single Sign On products	Ability to incorporate Enterprise Single Sign On products to include the provisioning solution within the Thick client single sign-on environment.	
8.6	Custom user authentication approach	Ability to incorporate custom user authentication approaches commensurate with internal security policies and to create private, filtered views of information about users and available resources.	
8.7	Ability to import and export configurations	Ability to import and export configurations to enable migrations between Development, Staging and Production environment without delays.	
9	**System Operations**		
9.1	interaction with target resources	Ability to interact with target resources without interfering with their performance.	

9.2	Operation for temp inaccessible system	Ability to continue to operate without degradation when the managed system is temporarily inaccessible.	
9.3	Function if provisioning solution unavailable	Ability for the managed resources to remain fully functional if the provisioning solution is unavailable	
9.4	Users interaction with provisioning solution	Responsiveness to users interacting with the provisioning solution features for searches, reporting, approvals, self-service and auditing.	
9.5	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.	
9.6	account and authorization information from existing systems	Ability to load account and authorization information from existing operational systems without data entry	
9.7	Reconcile accounts created by other adm. systems	Ability to detect and reconcile accounts created by, and/or changed by, other administrative systems (e.g., the local administration console provided with the managed resource)	
9.8	Support for configuration and scalability requirements	Support for configuration and scalability requirements for large environments and high- availability operations utilizing shared communication capacity on corporate WANs.	
9.9	End-to-end security	End-to-end security over account changes.	
9.10	Web-based functionality	Entirely Web-based functionality to allow easy distributed administration on an unlimited scale.	
9.11	Integrated functionality w/o duplicate data entry	Integrated functionality that does not require duplicate data entry or manual synchronization of information shared for multiple functions.	
9.12	Server configuration for high availability opn.	Ability for servers to be inexpensively configured for high-availability operation, including disaster recovery.	
9.13	Utilized data store configuration for high availability opn.	Ability for utilized data stores to be configured for high-availability operation.	
9.14	Accuracy in provisioning solution	Ability for provisioning solution to maintain accuracy when local administrators maintain privileges to make changes to target resources.	
9.15	Resilient communications design	Resilient communications design between distributed components to withstand network or target resource outages.	

9.16	Multi-layered security architecture	Multilayered security architecture for operation in a “demilitarized zone” ((DMZ) and for management of users and systems in untrusted environments.	
9.17	interaction with external systems	XML-based extensibility and interaction with external systems	
9.18	common and de facto standards	Use of common and de facto standards for interfaces that are internal and external to the provisioning solution.	
9.19	Integration of LDAP directory services	Integration of LDAP directory services as identity stores, access control system authorization stores and internal user account and policy stores.	
9.20	audit trails and system recovery	Inclusion of a persistent data store or repository for audit trails and system recovery.	
9.21	Quick response to user interactions	Ability to respond quickly to user interactions including report requests, access change requests, policy changes and password self-service.	

2.2. Technical specification for System Security Solution--

Requirement ID	Functionality	Description	Compliance by Vendor	Comments
Ss.1		**Audit Trails and Reports**		
Ss.1.1	Tracking key system accesses	The system must be capable of generating log trails, which contain details about any read /write access to sensitive data. Details must relate activity to an identifiable person. They must be configurable, so that filters and switches can be used to lower performance overheads and focus on areas of concern. It is important that the audit trail that is generated contain enough information to support after-the fact investigation of loss or impropriety.		
Ss.1.2	Time-stamp based auditing method	Where equipment uses a real-time clock to timestamp audit and other time related events, the clock should be regularly checked for synchronization with both connected systems and reference clock outside of the system, in this case the Indian Standard time. For daily reporting, this would ensure that the reports generated have some sanity given continuous data input		
Ss.1.3	Exception reporting	Where the security audit trail becomes unavailable for any reason, the system shall continue to operate but will trigger an alarm. Action shall be taken as soon as possible to rectify the situation		
Ss.1.4	Detailed system access tracking	System and application use and attempted use will be monitored to ensure that the integrity and security of the client and customer data is maintained. The documented process shall include details of: who will monitor what event and how, the		

		frequency of Monitoring, what to do when suspicious activity is noted, when to escalate and the escalation path. All events logged in the audit data shall be taken into account when deciding what to audit and the appropriate actions to take. The log must record the user or process responsible for the event, terminal ID where available, and the date and time of the event The following shall be monitored :- • Enabling and disabling of the audit process • Any changes to the type of events logged by the audit trail • Any changes to the audit trail itself •Start-up parameters and any changes to them • System or application start up and shut-down • Use of selected transactions • Changes to any of the database or records		
Ss.1.5	Maintaining audit trails	Audit records and journals shall be retained in a tamper proof environment in accordance with the Purchaser's policy for a reasonable amount of time to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.		
Ss.1.6	Disaster recovery	A recovery options analysis shall be carried out to produce the practical options for those systems and networks, which are deemed to require recovery in the event of a disaster. The most effective option shall be chosen, taking into account the cost of recovery and the cost to the business of unavailability of the application.		
Ss.2		**System Integrity**		
Ss.2.1	User process protection	The system should be able to protect the user process and local data from other user.		

Ss.2.2	Version consistency checks	Mechanisms should be in place to ensure that the currently installed software has remained consistent with the delivered product.		
Ss.2.3	Versioning	Software used on systems/ applications shall be subject to version and change control to ensure that only the current authorized software is used at all user location.		
Ss.2.4	Modification of the system	Modification or replacement of the software provided with the system would require special privileges		
Ss.2.5	System maintenance	Execution of system maintenance and repair software would require special privileges		
Ss.2.6	Basic checks on data input	Data input to an application shall be validated by the application to ensure that the data is correct and appropriate. As a minimum, an application shall check input data is complete. Within the required ranges, and contains no invalid characters. Procedures shall be established to deal with any input data violations.		
Ss.2.7	Time stamping modifications	The system should be able to track the date and time at which a resource was last modified.		
Ss.2.8 .	Integrity of data passed over a communication channel	The system should have in-built mechanisms e.g. checksums to verify the integrity of data passed over a communication channel.		
Ss.2.9	Data transfer lock	Where an encryption process used for data transfer fails and cannot be automatically corrected, then the transfer should not be completed.		
Ss.3		**Confidentiality**		
Ss.3.1	Use of encryption	The system should have the flexibility of encrypting the data stored online.		
Ss.3.2	Approval for cryptographic techniques	Any cryptographic techniques or encryption systems used to safeguard information shall have been approved by relevant authority on data security prior to their use.		
Ss.3.3	Approval for	Only security components which		

	security components	have been approved by the Purchaser shall be used to protect the Purchaser's sensitive information and processes.		
Ss.3.4	Documentation of encryption procedures	The procedures used to maintain confidentiality should be documented and access to them restricted.		
Ss.4		**Networking and Data Transfer**		
Ss.4.1	Authorized data transfer	All data transfers must be documented and authorized by the owner of the donor system. They must only be authorized where the receiving system has the capability to protect the data, i.e. it has an acceptable security rating.		
Ss.4.2	Inter system data transfers	Data which is to be passed between systems shall be labelled to indicate the type and sensitivity of that data. The security policy for a system will state what data may be sent to, or received from, another system and will state the translation, if any, between the labelling of the two systems. Interfaces that have been built - i.e. the data migration systems should have defined access rights. The interfaces should have a fixed enabling procedure - including the frequency with which the migration happens to and from the system, the data flow that would happen and the data items that would be frozen during such a migration.		
Ss.5		**Customer needs**		
Ss.5.1	Documentation of risks and its mitigation strategy	System developers responsible for customization should consider and document the risks and associated mitigation in the design.		
Ss.5.2	Installation and configuration	Developers will document instructions on how the system is to be delivered, installed and configured in a secure manner.		
Ss.5.3	Start-up documentation	Developers will document instructions for the secure start-up, re-start and operation of the		

		system.		
Ss.5.3	Start-up documentation	Developers will document instructions or the secure start-up, re-start and operation of the system.		
Ss.5.4	Interface designing	Interface designs must include the capability to selectively deny access to certain types of data.		
Ss.5.5	Scope control	Vendor supplied software packages must not be modified outside of the scope recommended by the Purchaser.		
Ss.5.6	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.		
Ss.5.7	Internal data	All applications shall be designed to minimize the risk of corruption by processing errors by building in validation checks, reconciliation checks etc., where necessary.		
Ss.5.8	Module and product testing	All new and modified software to be used on system/application shall first be tested by expert personnel to ensure that the software have been subjected to the rigor of test and thereby - a) Does not introduce added security risks b) Functions according to design specifications c) Does not adversely affect the operation of the system d) Introduces no unauthorized system changes.		
Ss.6		**Security of web services**		
Ss.6.1	XML based	As web services have certain		

	Web Security schemes	limitations with SSL type of security scheme, the web service technology shall be used with different XML-based security schemes. Some of the XML based securities include the following – • WS-security • XML digital signature • XML encryption • XKMS (XML Key Management specifications) • SAML (Secure Assertion Mark-up Language) • ebXML Message service The bidder shall ensure content security, message level security and secure message delivery, metadata security policy, trust management and secure public key infrastructure while Implementing web services using appropriate web security mechanism, which must be W3C/OASIS compliant.		

2.3 Technical specification for Firewall and NIDS Solution

Firewall and NIDS System		
Requirement ID	**Description of features**	**Bidder response Complied / Non complied**
1	**The firewall should have following features**	
1.1	State-full Packet Filtering - Should have a TCP State Aware Packet Filter Technology	
1.2	Appliance based Firewall shall have throughput of 5Gbps handling a minimum of 50000 simultaneous session per second & having Gigabit Ethernet interfaces.	
1.3	Firewall appliance should have 16 x 10/100/1000 Gigabit Ethernet interfaces.	
1.4	Support for unlimited number of users	
1.5	Network Address Translation - Should be able to provide Dynamic NAT as well as Static NAT	
1.6	Port Address Translation - Should provide capability to redirect the port requests to user configurable ports	
1.7	Integrated Security -Should have an inbuilt Anti-spoof engine to drop all such packets	
1.8	Firewall should support 1 Million concurrent firewall sessions	
1.9	Should drop all the IP fragment packets	
1.10	Should have Redundant power supply	
1.11	It should have 1TB of Total Hard Drive Capacity	
1.12	Should have protection against popular attacks such as ping-of-death attack, tear-drop attack, etc	
1.13	Administrator should be able to configure the default timeout for TCP/UDP services	
1.14	Should provide the capability to configure specific timeouts for specific services	
1.15	Should allow administrator to specify the maximum number of sessions between client and server	
1.16	Should log the number of active TCP/UDP sessions	
1.17	Should provide the firewall configuration backup and restore facility	
1.18	IP Traffic Control should be based on Source, Destination, Protocols, Ports, etc.	
1.19	Should provide administrative Access to the firewall management based on the AAA services provided by the TACACS+ and RADIUS protocols.	

1.20	Should provide different privileges for administration and management	
1.21	Should display firewall server's current date and time in remote Administrative Console	
1.22	Should be able to reconfigure the firewall parameters and policies from remote console	
1.23	Should provide Selective viewing of Logs based on Source, Destination, Source Port, destination port, rule number, time etc	
1.24	Should be able to Auto refresh the most recent logs while viewing	
1.25	Logs viewed through GUI Console should be traversable	
1.26	Should have support to work in high availability.	
1.27	Supports Message Digest Algorithm 5 (MD5)-based and plain-text routing authentication for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), preventing route spoofing and various routing-based DoS attacks.	
1.28	The firewall should be ICSA/EAL certified for firewall.	
1.29	The firewall should not create any bottleneck and performance problem.	
2	**The integrated Network Intrusion Detection and prevention system**	
	Platform	
2.1	Supports open source as an underlying OS.	
2.2	Monitoring Interface should be able to operate at layer 2.	
2.3	Minimum 8 10/100/1000 Ethernet monitoring interfaces should be provided.	
2.4	Should have in-built redundancy for storage, if applicable and power.	
2.5	Should have minimum throughput of 2 GBPS	
2.6	Should support High availability deployments either as active-active or active-passive or both	
3	**Security Content**	
3.1	Consists of vendor’s original threat intelligence and is not overly dependent on information available in the public domain.	
3.2	Is continuously updated with new threat intelligence, including detailed help text, in an automated fashion and without physical access to the unit.	
3.3	Security information is meaningful, comprehensive and freely available to customers and non-customers via a publicly accessible database	
3.4	Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
3.5	Detects and blocks zero-day attacks without requiring an update.	

4	**Customization**	
4.1	Requires minimal customization to built-in security checks	
4.2	Automatically blocks malicious traffic out of the box and allows additional blocking upon policy customization. • Can enable/disable each individual signature. Each signature should allow granular tuning.	
4.3	Allows users to control the number of times a sensor notifies the console when a flood-type attack occurs.	
4.4	Supports assigning of ports to custom applications. In order to monitor any type of port traffic, the user should be able to assign a service to a port, label that port with a custom name, and then monitor that port for activity	
5	**Updates**	
5.1	Supports automated security check and product updates.	
5.2	Updates are frequent and regular	
5.3	Security check updates do not require reboot of IPS unit	
6	**System Integrity**	
6.1	Supports encrypted communication between all components	
6.2	All communications should be encrypted. It should have a built-in mechanism to ensure that only legitimate users have access to the agents and to the security information stored in the database.	
6.3	Supports multiple user roles. These roles should allow or deny specific privileges to users. Privileges should include a range of management and viewing or reporting capabilities. Additionally, access to specific agents and/or assets should be controlled, thus allowing only certain users access to particular computers, regardless of the privileges provided by virtue of their role.	
6.4	Supports system management hierarchy and associated access. The system should allow different groups within an organization to maintain their own console while at the same time allowing a central security team the ability to view all events across the entire enterprise	
6.5	Has remote log storage capability to support logging to a central repository. In the event that the log data is sent from the IDS to a separate Management server, the IP address, or any other unique identifier of the IDS shall be captured with the other recorded log data for the logged events.	
7	**Performance Considerations**	
7.1	Does not introduce network latency. Provide independent validation.	
7.2	Fails open should a Power loss/Ethernet/hardware/software failure occur.	

7.3	Notifies console of unit interruption. Console should receive alert and/or provide additional notification to administrator should any component become non-operational or experience a communications problem. The alert should specify the type of problem encountered, and users should have the ability to enable tracing mechanisms to determine the exact nature of the issue.	
8	**Accuracy**	
8.1	Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks	
8.2	Accurately prevent intrusions from occurring	
8.3	Accurately respond to intrusion attempts.	
8.4	Resistant to evasion techniques.	
8.5	Accurately identifies attacks with correct severity level while allowing benign traffic to pass without interruption.	
9	**Detection Technology**	
9.1	Detects and blocks all known, high risk exploits.	
9.2	Employs full seven-layer protocol analysis of over entire range of TCP/IP internet protocols. Performs stateful packet inspection.	
9.3	Decodes backdoor communications / protocols regardless of port.	
9.4	Security checks have a pre-defined severity level associated with them. The severity of each check should also be configurable	
9.5	Detects and blocks malicious web traffic on any port	
9.6	Does TCP stream reassembly.	
9.7	Does IP defragmentation.	
9.8	Detects attacks within protocols independent of port used.	
9.9	The detection engine should be able to detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol. For example, it should be able to detect HTTP	
9.10	Traffic running on a port other than port 80 and then start monitoring that data stream for HTTP attacks. Additionally, users should be able to customize the ports associated with any protocol or application so that the IPS automatically monitors those ports	
9.11	Supports attack recognition inside IPv6 encapsulated packets.	
9.12	Performs real-time event consolidation of multiple events at sensor	
10	**Prevention Technology**	

10.1	Supports active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs.	
10.2	Supports active blocking of traffic based on dynamic responses to pre-defined rules.	
10.3	Allows definition of network level filtering rules based on source and destination IP and/or network, and source and destination IP ports.	
10.4	Supports several prevention techniques including drop packet,TCP-RST etc.	
10.5	TCP-RST etc.	
11	**Response Mechanisms**	
11.1	Supports granular set of unique responses for every signature	
11.2	Supports response adjustment on a per signature basis.	
11.3	Offers a variety of built-in responses like console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures.	
11.4	Is able to dynamically alter the severity of an event based on event validation features that add vulnerability state information to an alert to reduce false alarms while blocking truly malicious activity?	
11.5	Allows automatic responses based on event validation.	
11.6	Allows user-defined responses. Must support custom responses such as the execution of a command-line script	
11.7	Must be able to transfer all relevant event data to the user defined program such as source and destination IP address, ports, attack type, event name, date and time stamp, etc.	
11.8	Supports integration with other alerting mechanism or software that can generate paging or SMS response.	
12	**Certifications**	
12.1	NIDS/NIPS should be NSS/Tolly/JD Power-SCP/EAL approved	
13	**Management – Agent Command and Control**	
13.1	Management platform supports command, control, and event management functions for NIPS, NIDS.	
13.2	Allows central management of signature updates. Is able to centrally push out updates from one location to multiple IDS installed across enterprise.	
13.3	Supports central management of policy configuration	
13.4	Management platform includes an automated deployment	
14	**Management – Reporting**	

14.1	Includes built-in reports. The console should be capable of producing graphical metrics and time-based comparison reporting. The information in the reports should be available for a group of assets, an entire Site, or an entire enterprise. Further, users should be able to drill down into these graphical reports to view pertinent details	
14.2	Built-in reports should include high level summaries and detailed reports.	
14.3	Supports the creation of custom reports, preferable without the user having to learn a third party reporting system.	
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	
14.5	Can schedule reports for automatic generation to all supported formats.	

2.4. Technical specification for Antivirus solution

Anti-Virus Solution		
Requirement ID	Description of feature	Compliance
1	Technical Specifications for Antivirus at desktops & servers	
1.1	The antivirus solution should provide enhanced antivirus protection for desktops & servers.	
1.2	Should have a Centralized Management Console	
1.3	Should be a Single, Configurable Installation with centralized configuration & policy management.	
1.4	Should have a Common Distribution Mechanism via combination of push & pull Technology for better BW management	
1.5	Should have logical group based on IP addresses (Subnets). Should support integration with Active directory for directory structure of computers for better management	
1.6	Should be support Multi-Platform OS Support	
1.7	Should support Policy Enforcement	
1.8	Should have Common, Extensible Scanning Engine	
1.9	Should have Configurable Scanning. Should have the ability to control the amount of CPU resources dedicated to a scan process	

1.10	Should have Unknown Virus Detection & Repair. Should have behavioral & Heuristic scanning to protect from unknown viruses. Should have buffer overflow protection integrated with AV scan engine for protection from threats/exploits that uses buffer overflow vulnerability regardless of presence of signature / OS patches	
1.11	Should have Compressed File Detection and Repair	
1.12	Should have Research Centers for proper updates as well as technologies to support the outbreak	
1.13	Should have 24*7 Global Technical Support	
1.14	Should ensure security policy enforcement by integrating and centralizing installation, deployment, management & updating	
1.15	Should conserve n/w b/w by updating virus definitions with incremental updates. Should support daily update for definition files. Size of daily update should be optimal and in the range of 10-12MB	
1.16	Should be able to support the Platforms of desktops and servers of the utility	
1.17	Anti-Virus Software must have the capability to detect and clean Virus	
1.18	Should be able to detect new classes of viruses by normal virus definition update mechanisms	
1.19	Should provide common definitions for all operating systems supported & across all product ranges.	
1.20	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.	
1.21	Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.	
1.22	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.	
1.23	Should allow for incremental virus definition and scan engine updates.	
1.24	It should recognize a missed event on a machine, which was switched off, and restart the same when machine is turned on.	
1.25	The anti-virus software should be able to automatically detect and update definitions and scan engine form the nearest Distributed repository in the network.	
1.26	Should be able to set and monitor client server configuration remotely.	
1.27	Should be able to lock down all anti-virus configurations at the desktop.	
1.28	Should be able to optionally make the client user interface invisible for transparent protection.	
1.29	User should be prevented from being able to uninstall the anti-virus software.	

1.30	Must be able to distribute new and update anti-virus software, virus definitions and configuration files automatically to clients and servers from a central location (Clients need not login to the central server to download the updates)	
1.31	Should be able to view all servers and clients from one console.	
1.32	Should be able to initiate virus sweeps remotely (central command to scan all machines in case of an outbreak Should support folder/directory/share lockdown centrally to contain virus outbreak. Should support blocking of files based on their name to stop spreading of new viruses whose signatures are not released. Should support port blocking for unknown processes (e.g. port 25 is blocked for every process except Outlook.exe). Should support to automatically block traffic coming to a clean system from malicious / infected system)	
1.33	Should be able to perform manual or scheduled virus scans on individual computers remotely.	
1.34	Must provide centralized event logging to locate and cure virus problems.	
1.35	Alerts on virus activity should be passed on to administrator	
1.36	OS INSTALLER SUPPORT- should be incorporated for a standards-based installation. Should support installation of software package in both format OS Installer & EXE file	
1.37	Should enables administrators to identify which machine has generated a threat that is spreading by an open file share (for example, Nimda or CodeRed).	
1.38	Should enable administrators to easily move clients (who have changed departments, for example) from one physical parent server to another simply by dragging and dropping through the central management console.	
1.39	Should store event data generated while a client is disconnected from the corporate network and forwards it when the client reconnects.	
1.40	Should enables administrators to launch an immediate LiveUpdate session on single or multiple clients during an outbreak.	
1.41	Should enable administrators to select the events that clients forward to their parent servers and those secondary servers forward to primary servers.	
1.42	Should extends virus, worm, and Trojan horse detection capabilities to include certain non-virus threats, such as Sypware, Trackware, Adware, Dialers, Joke Programs, Remote Access, and Hack Tools, which can be used with malicious intent.	
1.43	Should scan the body text and attachments of incoming e-mail messages that are delivered through POP3 / IMAP / MAPI mail clients	
1.44	Auto Protect should be loaded on system startup, and then unloaded on system shutdown to help protect against viruses, such as Fun Love.	

1.45	Should scan in-memory processes on disk for threats. If a threat is detected, the running process can be terminated	
1.46	Should have enhanced protection from Spyware and Adware, including: Real-time protection to reduce the risk of Spyware reaching the system.	
1.47	Should automatic remove Spyware and Adware for easy disposal of security risks.	
1.48	Should have Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find Spyware infection.	
1.49	Should have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures.	
2	**ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP**	
2.1	Should use a multi-layered anti-spam approach to combine various blacklisting and white listing techniques, as well as heuristic detection to stop spam at the earliest point of network entry providing maximum detection with minimal false positives.	
2.2	Should dynamically analyze and tag spam messages by appending custom text, e.g. “SPAM”, to the subject line. Should provide a high degree of reliability in detecting spam messages, especially compared to traditional content filtering techniques.	
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.	
2.4	Should enable administrators to exclude known and trusted domains from real-time blacklists and heuristic scanning.	
2.5	Should allow administrators to manually block e-mail from specified user addresses, as well as entire domains.	
2.6	Should block e-mail messages based on subject line, attachment name, and maximum message size, specific keywords with regular expressions.	
2.7	Should prevent external sites from bouncing or relaying messages through your customers’ mail servers.	
2.8	Should detect non-standard MIME messages that contain malicious content.	
2.9	Should use any and multiple DNSBL-based blacklist services to stop spam based on source.	
2.10	Should customize domain/address block lists to prevent delivery of e-mail messages from specific senders or domains.	
2.11	Real Time Status Monitoring- Should be able to view all email performance metrics with the click of a button, providing the number of messages processed, the number of messages in queue, the number of spam mails detected, blocked, Viruses detected and blocked etc	

2.12	Should have mechanism to detect and block different threats like polymorphic viruses, Blended Viruses	
2.13	Should include an inbuilt SMTP server so that it can transparently reside behind firewalls or SMTP gateway	
2.14	Should support Global as well as user defined blacklists.	
2.15	Should have support for user specific custom whitelists and blacklists.	
2.16	Should support spam based filtering rules.	
2.17	Should support multiple levels of spam score thresholds. And Administrators can define specific handling rules based on these different spam scores	
2.18	Should have an X-bulk header (an optional header that is generally not shown to the end-user) can be inserted into suspected spam messages, and serves as a description for an action taken on an email.	
2.19	Detect non-standard MIME messages that contain malicious content.	
2.20	Should protect against new virus classes that traditional virus definitions alone cannot address. The engine updates should be automatically applied as administrators download new virus definitions—without stopping or restarting scanning services.	
2.21	Should have central server management for virus and Spam mails. The central server should have web-based GUI for administrators to access these quarantine mails for further inspection	
2.22	Should support comprehensive activity logging Keeps track of virus activity on customer networks by logging: - System actions (logins, logoffs, virus définition updates) - Message actions (accepted, rejected, bounced, delivered, delivery failures, completed) - Virus actions (repaired, deleted, quarantined)	
2.23	Should support a dedicated quarantine manager to handle a large number of mail environments, while the scanning engine is dedicatedly scanning the malicious mail traffic	
2.24	Central Quarantine manager should support multiple mail gateways. Should provide web based GUI to the end user for their own quarantine mails management	
2.25	Operating System of the appliance should be hardened to protect itself from any unnecessary services or traffic.	
2.26	Solution should support Bayesian filtering of mails	
2.27	Solution should support lexicons for compliancy like – Data Privacy, HIPAA	
2.28	Solution should support Policy based mail routing	
2.29	Solution should support TLS encryption for secure communication	
2.30	Solution should support mail traffic coming from different VLANs based Vlan ID	
2.31	Solution should support client tool for submission of spam mails directly from Mail/messaging solution. Solution should support spam learning through user mail submission	

2.32	Solution should support multi level of actions on quarantine mails	
2.33	Solution should support spam scanning on PoP3 protocol as well	
3	**TECHNICAL SPECIFICATIONS FOR GATEWAY ANTIVIRUS FOR HTTP & FTP**	
3.1	Should have combined Antivirus and Content Filtering Technologies at the Gateway high performance, one-time scanning of all incoming and outgoing HTTP / HTTPS and FTP traffic. Should provide high performance and one time scanning of http & ftp traffic for virus and content filtering	
3.2	Should let you export URL Filtering's extensive, web-based reports to a comma-separated (CSV) file for easy import into programs like Crystal Reports or Excel for creating flexible graphical reports.	
3.3	Should resides behind firewalls, so it is transparent to users and should not impact network performance	
3.4	Should filter Internet content, using extensive, pre-defined category lists (such as crime, sex, gambling, and intolerance) to get you up-and-running quickly	
3.5	Should go beyond simple list-based filtering to provide multilingual, real-time filtering technology that reviews Web documents on the fly, without performance degradation. Should examine Internet content based on the threat in terms of viruses, Trojans, spam, & should block those web sites	
3.6	Should control Internet access by time of day and day of week, allowing users to access work-related sites during business hours and providing open Internet access during lunch or after hours	
3.7	Should Offer a flexible policy management interface to make setting guidelines for users, groups of users, or system-wide users intuitive and easy. For example, you can specify: Allow lists, which focus users' Internet access on specific sites (e.g., shipping)	
3.8	Should support user authentication based on Windows NTLM, Kerberos and LDAP. Should also support transparent authentication for Windows domain users	
3.9	Should monitor users' Web access through feature-rich reporting—increasing your awareness of all Web activity within your organization and helping to deter non-work-related surfing. Should also allow you to export data into a CSV file format for viewing. Tracks all: Content and access violations / Search engine requests/Auto Locks. Provides valuable summary reports, which identify: Top ten Web sites/ The most active users / Cache/hit ratio / Frequency and types of violations	

3.10	Should provide rich reporting on the user activity for web and URL filtering. Should have reports for Top URL blocked, Top Users, Executive Summary reports etc	
3.11	Should allow organizations that choose not to restrict employees' Internet access to monitor and report on all Internet traffic unobtrusively—still keeping them informed of their organizations Web activities and deterring inappropriate or unproductive Web surfing	
3.12	Should use Access Scheduling to control Internet access by time of day and day of week, helping to: 1) Curb high-bandwidth Internet usage during peak hours of demand—freeing limited resources for those that need it most. 2) Ensure your IT investment is used wisely. 3) Caches frequently requested documents, reducing network traffic	
3.13	Should offer an HTML-based interface that lets you configure and manage URL Filtering from any Web browser, from any location—making administration a snap	
3.14	Should be an appliance based solution with hardened OS thus making it easier to manage & fit into any infrastructure	
3.15	Should enable administrator to manage multiple appliances from single Management console for policy, configurations and reporting.	
3.16	Solution should support blocking of specific files getting downloaded from web sites	
3.17	Should integrate with multiple LDAP servers to create policies based on User groups	
4	**TECHNICAL SPECIFICATIONS - ANTIVIRUS PROTECTION FOR EMAIL Application**	
4.1	Should support latest windows operating system and application server.	
4.2	Should provide a comprehensive solution consisting of multi-level anti-spam, rules-based content filtering and antivirus.	
4.3	Should be able to control spam more effectively by having multiple score assignment to every spam message with heuristics anti-spam detection	
4.4	Should allow messages to be handled appropriately based on the heuristics-assigned spam score with multiple spam disposition options.	
4.5	Should incorporate intelligent, rules-based content filtering to prevent unwanted content from entering and confidential information from leaving the network.	
4.6	Should minimize false positives by creating a trusted sender Whitelist.	
4.7	Should bypass heuristic anti-spam & RBL (Real-time Blacklist) for certain recipients with recipient Whitelist.	
4.8	Should eliminate the entire message automatically with Mass Mailer Cleanup, not just attachments generated by mass mailer worms.	

4.9	Should update automatically with new virus definitions from internet to keep your protection up-to-date.	
4.10	Should protect against new viruses without requiring re-installation of software, helping to reduce the cost of ownership.	
4.11	Should automatically filter out emails with inappropriate attachment names, extensions, or content, reducing traffic on your Microsoft Exchange servers	
4.12	Should have an alternate to automatically update all of the Microsoft Exchange Servers from an internal virus definition server that will pick up updates from internet.	
4.13	Should provide immediate protection for new mailboxes and public folders.	
4.14	User/Group Based Rules - User/Group based rules should provide the ability to assign rules to only apply to a certain group of users or create global rules with exceptions. Users and groups can be taken from active directory or they can be entered using full email addresses or wild cards	
4.15	Attachment Content Scanning – Should scan for content contained within most file types including Microsoft Office documents, Adobe Acrobat, text, RTF, and database files.	
4.16	True-file Typing for Multimedia and Executables – Should block/Quarantine multimedia and/or executable files based on true file type (regardless of file extension). One of the following dispositions should be applicable: delete attachment, delete message, quarantine file, or log only	
4.17	Simplified Content Rule Interface – The interface for creating content filtering rules should ease the process of creating custom rules. Match lists should be added and edited within the content filtering pages. Rules should include content to match on and exceptions within the interface to better display the intent of a rule	
4.18	Generate Reports across Multiple Servers— Should kick-off reports on each individual server from a central location and then browse to individual servers to view the report	
4.19	Should be able to view a summary of activity and information for all Microsoft Exchange servers that are managed within a group, including consolidated spam and anti-virus data, from the home page.	
4.20	Expanded Protection against Security Risks— Should have the ability to detect expanded threats such as joke ware, Spyware, Adware and other non-viral risks. Separate dispositions should be applicable to detected security risks including delete file, delete message, quarantine and log-only	
4.21	Auto-generated Summary Reports— Should create a summary report of all activity on a single Microsoft Exchange server, and automatically generate the report at a given date and time.	
4.22	Auto-generated Email Report– Once a report is generated; it should be automatically delivered to specified recipients.	
4.23	Graphical Reports– Reports should be generated that include charts and graphs to provide a clear picture of virus, filtering, and spam activity within an organization.	

4.24	Should have different log database for detection event and product. Should provide multiple scanning options like – proactive scanning, Background scanning, Transport level scanning. Should provide scanning of nested archived files for at least 30 times	

2.5. Technical specification for Reverse proxy

Feature	Specifications	
Hardware	The solution may be a software based i.e. no appliance should be used to propose the solution and solution should be independent deployed on any server hardware based platform.	
Web Threat Protection	The solution should provide forward proxy, reverse proxy, caching, on box malware inspection, on-box AV scanning, SSL inspection/encryption.	
	A reverse proxy should distribute the load from incoming requests to several servers, with each server serving its own application area.	
	The solution should have gateway level AV and malware protection on same hardware	
	The solution should be able to perform SSL inspection to detect and block malicious content downloaded through SSL and also blocking sensitive information uploaded to SSL websites.	
	The solution should have range based IP spoofing to provide accurate representation of the IP addresses as it exits the proxy. Also solution should have capability to monitor mirrored outgoing traffic and send resets for protocol traffic as required.	
Administration, Authentication and Policy Controls.	The management console provides Security administrators with a comprehensive, up-to-date view of threat characteristics and response, user activity, network load, system stats and more.	
	The solution should have authentication options for users/groups, It should supports authentication of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), and LDAP.	
	The solution should pre-built report templates which the administrator can use for generating reports.	
	The solution should support custom report creation in Excel and PDF.	
	The solution should be able to consolidate reports from multiple boxes for centralized logging and reporting.	
	The solution should provide detailed information on security incidents to comprehensively investigate individual threat events	
	The solution should provide a Web UI to manage Internet usage policies, it also should support delegated administration and reporting capabilities so different roles can be created to manage policies and view reports.	
	The solution should provide native system health monitoring, alerting and troubleshooting capabilities.	
	The solution should provide reports based on hits, bandwidth and browse time.	

	The solution should support automatic download of available patches or fixes	
	The Solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report.	
	The OEM should have own TAC center in India.	
APT Capabilities	The solution must provide malware, anti-virus, anti-bot etc scanning though in-built AV scanning engine in appliance also Solution should provide APT (apt feature should be enabled through license upgrade as required), Advanced threat protection capabilities over web channel with sandboxing functionality enabled through license upgrade.	

3. Bill of material

S.NO	Item	Quantity		User License
		Data Centre	DR	
1	**Supply and implementation of Firewall. (Hardware + Software)**	1	Hardware - 1 Software - should be a part of Data Center / DR license.	Unlimited
2	**Supply and implementation of NIDS (network intrusion detection and prevention system. (Hardware + Software)**	2	Hardware - 2 Software - should be a part of Data Center / DR license.	1000-1100
3	**Supply and implementation of anti-virus for Workstations and Servers Solution (Software)**	1	Should be a part of Data Center / DR license.	1000 – 1100
4	**Supply and implementation of anti-virus for SMTP Gateway. (Software)**	1	Should be a part of Data Center / DR license.	1000 – 1100
5	**Supply and implementation of anti-virus for HTTP, FTP Gateway. (Software)**	1	Should be a part of Data Center / DR license.	1000 - 1100
6	**Supply and implementation of anti-virus for Email gateway. (Software)**	1	Should be a part of Data Center / DR license.	1000 – 1100
7	**Supply and implementation of Reverse proxy. (Software)**	1	Should be a part of Data Center / DR license.	Users -1000 – 1100 Servers - 50
8	**Supply and implementation of Identity and access management solution. (Software)**	1	Should be a part of Data Center / DR license.	1000 – 1100
9	**Supply and implementation System security solution. (Software)**	1	Should be a part of Data Center / DR license.	1000 - 1100

4. Timelines for Delivery and Installation

Bidder is required to deliver the equipment at the specified locations / offices within 4-6 weeks from the date of the Release Order.

Supplied equipment should be installed in 4 weeks from the date of delivery.

5. Payments Criteria

The payment will be done on milestone basis for IT security Solution system as given below:

S No	Milestone	Payment
1	On successful supply of material with all accessories, installation, commissioning, testing and Integration of IT Security Solution (Hardware + Software), user acceptance for Solution, Completion of trainings and acceptance by RECPDCL Nodal Officer. The bidder is required to obtain user acceptance from RECPDCL Nodal Officer and submit a copy of user acceptance to the designated Authority along with the invoice.	70% of Entire Contract Value (excluding AMC (O&M) cost)
2	After 02 month of "Full Roll out and Go live of all towns", loading of all applications, system testing with at-least 99.8% performance and acceptance of System by Goa Electricity Department. The bidder is required to obtain user acceptance from RECPDCL Nodal Officer and submit a copy of user acceptance to the designated Authority along with the invoice.	30% of Entire Contract Value (excluding AMC (O&M) cost)
3	AMC (O&M) of IT Security Solution for 2 Years after implementation period.	On quarterly basis in arrears, i.e. at the end of every quarter.

7. Penalty

LD/Penalty as mentioned in GCC as mentioned in Annexure-VII

6. SLA for System security (H/w and S/w)

a. Terms of Agreement:

This agreement shall remain in force from the date of commencement i.e. <date > till the expiry of the contract (including extension if any). Commencement of Service Period:

- Warranty will start after successful installation & acceptance testing from user. Comprehensive warranty for period of 5 years for the IT security solution.
- OEM should support in case of non-compliance by bidder.
- SLA Based Support through telephone/Fax/E-mail/ personal visit.

b. Support

- Vendor will provide support on calls lodged by the user.
- Vendor shall provide support service for a period 5 years for the system security solution (Hardware and software) as per terms and conditions laid in this document.
- Support should be available on 24 x 7 basis.
- Escalation matrix to be provided with the bid.
- Study and redesign network security in consultancy with user.
- Prepare landscape/diagram and deliverable SOW.
- Installation, implementation and documentation of the same.
- Provide hands-on training for concerned teams.
- Vendor should complete the project as per agreed timelines.
- A copy of agreement between service provider & OEM should be provided to user.
- Services:
  - **a) Uptime guarantee:** The agreement stipulates that vendor shall maintain the system with uptime of 99.8%. The uptime will be calculated on monthly, peak and non-peak basis. This excludes any kind of down time taken for preventive maintenance.
  - **b) Maintenance Services:** Vendor shall provide maintenance services under this agreement for the solution on par with OEM's service standard.
    The maintenance services shall include the following: -

i. Corrective Maintenance:
Any system failure will be attended by vendor's engineer and if necessary by their specialists.

ii. Preventive Maintenance
User will allow vendor to carry out required Preventive Maintenance on the provided solution. The down time required for Preventive Maintenance will be communicated to user by the vendor. Vendor will prefer to execute preventive maintenance work during non-business hours.

iii. Movement of devices
It is vendor's responsibility for any Hardware movement across sites till the order expires.

c) Spares Availability/ Support from OEM
Vendor shall have a back-to-back Business Critical Support arrangement with the OEM partner for spares and escalation support. Vendor shall also have a formal arrangement with OEM for any technical support that may be required on the hardware or software. OEM letter for support is to be submitted against RO.

Deliverables under system software/patches support include:
a) System software updates
b) Pro-active patch notification and installation on equipment
c) OS bug fixes
d) Access to OEM diagnostic solution database

d) Response Time and Resolution Time :

i. 2 Hour Response Time (24x7)
ii. 4 Hours Resolution Time (Including Response Time)

c. Reporting

The vendor shall prepare a monthly Report in the User prescribed format covering the following:

- Uptime summary report
- Preventive maintenance report

The vendor will enclose uptime report along with the bill for certification.

d. Method of contact to the engineer

Vendor should provide the contact number, e-mail ID and name of the concerned engineer.

e. Level of specialist assistance to the engineer

The vendor will ensure that all required specialist/technical support will be provided to his engineer so that the guaranteed uptime will be achieved on monthly basis.

f. Level of escalation

- Level I: Account manager <Contact no.>
- Level II: General manager or equivalent level < Contact no.>
- /Level III: CEO of the company < Contact no.>

g. Penalty for SLA Non-Compliance

In case the uptime commitment is not met, same shall attract a penalty @ Rs. 10,000 per day. The penalty amounts shall be recovered from the payments due to the vendor. A sample calculation is given below:

If the actual uptime achieved in 97.5%, penalty amount shall be:

Rs. 10000 x {(99.8 - 97.5) / 100 x 365} = Rs. 83,950

SECTION-V

GENERAL CONDITIONS OF TENDER

Part – 1

1. The bidder must fulfil the above eligibility criteria/pre-qualifying conditions for evaluation of their bids. Bids of bidders fulfilling the above eligibility/pre-qualifying conditions will only be evaluated by the duly constituted evaluation committee. Bids of the bidders not fulfilling the eligibility/pre-qualifying conditions given above may be summarily rejected. Undertaking for subsequent submission of any of the above documents will not be entertained under any circumstances.
2. RECPDCL reserves the right to conduct the reverse auction (if required) for the products/ services being asked in the tender. The terms and conditions for such reverse auction event shall be as per the Acceptance Form attached as Annexure B of this document. The bidders shall mandatorily submit a duly signed copy of the Acceptance Form along with the tender document as a token of acceptance. In case of denial for participation, bidder shall not be entitled for any kind of claim.
3. RECPDCL reserve the right to verify/confirm all original documentary evidence submitted by the bidder in support of above mentioned clauses of eligibility criteria, failure to produce the same within the period as and when required and notified in writing by RECPDCL shall result in summarily rejection of the bid.
4. Engagement with RECPDCL does not confer any right to the agencies to be invited for participating in any bids, tender etc. floated by RECPDCL. RECPDCL reserves the right to call bids/assign work/associate the agency/agencies in any area as may be deemed fit by RECPDCL depending upon the profile provided by the agencies and requirement of assignment.
5. RECPDCL reserves the right to accept or reject any or all requests for engagement without assigning any reason or to accept in parts and engage more than one agencies at its sole discretion.
6. Acceptance of the application(s) constitutes no form of commitment on the part of RECPDCL. Furthermore, this acceptance of the application confers neither the right nor an expectation on any application to participate in the proposed project.
7. RECPDCL reserve the right to waive off any shortfalls; accept the whole, accept part of or reject any or all responses to the Tender.
8. RECPDCL reserve the right to call for fresh tenders at any stage and /or time as per the present and /or envisaged RECPDCL requirements even if the tender is in evaluation stage.
9. RECPDCL reserve the right to modify, expand, restrict, scrap, re-float the tender without assigning any reason for the same.
10. The responder shall bear all costs associated with the preparation and submission of its response, and RECPDCL will in no case be responsible or liable for these costs, regardless of the conduct or the outcome of the tender process.
11. Consortium and joint venture responses are not allowed, in any case.
12. **Performance Security:**

    1. The agency need to deposit within fifteen (15) working days from the date of acceptance of work order, a Performance Security in the form of Bank Guarantee or Demand Draft (DD), for an amount of 10% (Ten per cent) of the Tender value against the supply portion for 3 years plus 6 month claim period and after completion of 3 years or before expiry of PBG of supply portion bidder has to submit the PBG for AMC portion for 2 years plus 6

month claim period of 10% of total value of AMC portion for the due performance and fulfilment of the contract by your firm in the format placed at Annexure – A.

2. The Performance Bank Guarantee may be drawn from a scheduled commercial bank in favour of The "REC Power Distribution Company Ltd", New Delhi.
3. The Performance Bank Guarantee may be discharged/ returned by the RECPDCL after the completion of the contract upon being satisfied for the performance of the obligations of your firm under the contract.
4. Failing to comply with the above requirement, or failure to enter into contract within 30 days or within such other extended period, as may be decided by the CEO, RECPDCL shall constitute sufficient grounds, among others, if any, for the annulment of the award of the tender.
5. In the event the firm being unable to provide the services, during the engagement period as per the contract for whatever reason, the Performance Bank Guarantee would be invoked by RECPDCL.
6. No Bank Charges/ interest shall be payable for the Performance Bank Guarantee.

13. Rates and Prices: Bidders should quote item-wise rates/prices including all taxes, duties except Service Tax for courier service of different stations mentioned in Form-III.

a All statutory duties and taxes (including excise and customs) Sales Tax and other charges will be payable by the bidder.

b Price quoted by bidder shall be firm excluding service tax for contract period.

c Price quoted shall be firm and any variation in rates, prices or terms during validity of the offer shall require forfeiture of the EMD.

14. In case of default in your services or denial of services, RECPDCL, at its sole discretion, will be free to avail services of other courier service providers at your "Risk & Cost".

15. All other terms and conditions of the GENERAL CONDITIONS OF CONTRACT as attached in Annexure shall be applicable.

16. In case of continued non-satisfactory performance, RECPDCL have the right to withdraw the work & get completed the work at the risk and cost of the agency. Further the agency may be blacklisted for a period of one year or more for participating in any of the bids invited by RECPDCL. Also, RECPDCL would be free to intimate such black listing to various state/central utilities/ Ministry of Power/State Governments/other agencies not to consider the said agency for any assignment including of the same on websites.

17. In a tender either the Indian agent on behalf of the Principle /OEM or Principle / OEM itself can bid but both cannot bid simultaneously for the same item/product.

18. If an agent submits bid on behalf of the principal /OEM, the same agent shall not submit a bid on behalf of another principal /OEM in the same tender for the same item/product.

1. The bidder needs to provide details of their Locations in India in the following format.

Firm Detail – List of Locations in India

No.	Location Address	State	City	Contact Person	Contact Details
					Phone No: Email Id:

SECTION-VI
ELIGIBILITY CRITERIA

Pre-Qualifying Criteria (Mandatory Requirements) for OEM

S. No.	Qualification Criteria	Documents Required
1	The OEM vendor shall have ISO 9001:2008 and ISO 14001 certifications	Latest ISO certificates
2	The OEM vendor shall have an annual turnover more than INR 100 crores from hardware business in each of the last three (FY 2012-13, 2013-14, 2014-15) financial years.	Last three years audited balance sheets and Profit and Loss Accounts Statements Self-certify + CA certificate
3	The OEM vendor shall have at least one service/support center within the Goa or nearby (Karnataka & Maharashtra) State with sufficient infrastructure.	Self-certify along with location of service center
4	Require OEM certificate for 5 years support that in case the bidder is unable to supply equipment and provide services, the OEMs will provide back to back arrangement for critical support and spares for at least 5 years.	On OEM letterhead duly signed and stamped
5	The bidder needs to submit OEM certificate for ensuring that OEM has certified the bidder to supply the equipment and provide necessary services.	As per MAF Form V

Pre-Qualifying Criteria for Bidder

1. The bidder shall be a private/public Company registered under Company Act 1956. Certificate of Incorporation and Registration needs to be submitted along with the bid.

2. The bidder shall have a minimum annual turnover of 2 crore in each of the last three (FY 2012-13, 2013-14, 2014-15) financial year. The Audited financial reports and copy of the certificates supporting the above need to be submitted as proof.

3. 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.

Or

b. Two projects each covering supply, installation, commissioning and testing of IT security Solutions of equal or more than value of Rs. 1 Crore.

Or

c. Three projects each covering supply, installation, commissioning and testing of IT security Solutions of equal or more than value of Rs. 80 Lakhs.

Details of Successful Completion of Projects by Bidder

Financial Year of Completion	Equipment Supplied	Number of Units Supplied	Company Name and Location of Project

SECTION-VII

TENDER EVALUATION METHODOLOGY

OPENING OF BID:

The Bidder or his authorized representative may be present at the time of opening of bid on the specified date, but a letter in the form annexed at (Form – I) hereto must be forwarded to this office along with bid and a copy of this letter must be produced in t h e office by the person attending the opening of bid. Unless this letter is presented by him, he may not be allowed to attend the opening of bid.

In case of unscheduled holiday on the closing/opening day of bid, the next working day will be treated as scheduled prescribed day of closing/opening of bid; the time notified remaining the same.

EVALUATION OF BID

PRE-QUALIFIYING CRITERIA - Evaluation and comparison of bids will be done as per provisions of Pre-qualifying Criteria supporting documents as proof of pre-qualifying criteria at section – VI.

The RECPDCL will examine the bids to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed and whether the bids are generally in order qualifying to which bids shall be summarily rejected.

PRICE EVALUATION CRITERIA

1.1 Bidder should quote their rates/prices in Indian Rupees only which shall be inclusive of all applicable taxes, duties, levies, insurance, transportation etc., applicable excluding service tax for entire scope of work as per Price Schedule included to Form - III of this tender document.

1.2 Bids shall be evaluated on the basis of the total evaluated value as per the quoted rates for the services mentioned in Scope of Work. The total evaluated price as per the evaluation methodology mentioned as under at Form - III of this tender document and the other details mentioned therein will be the basis for the evaluation purposes and for arriving at inter-se ranking of the various bidder of the tender.

1.3 Bid shall be evaluated through as per the Performa of Schedule rate, i.e. Form-III, which shall be filled by the bidder as a Financial Bid.

1.3 AWARD CRITERIA

The purchaser will award the contract to the successful bidder whose bid has been determined to be in full conformity to the bid documents and has been determined as the lowest evaluated bid.

REC Power Distribution Company Limited

FORM-I

Letter for Submission of Tender

To,
Addl. Chief Executive Officer
REC Power Distribution Company Ltd.,
1016-1023, 10th Floor,
Devika Tower,
Nehru Place, New Delhi-110019

Sub.: Engagement of bidder for Supply and installation of IT Security Solution (Hardware and Software)

Sir,

1. With reference to your Tender No. ---------- dated ---------- for **Purchase of System security solution(H/w and S/w),** I wish to apply for engagement with RECPDCL as "**Purchase of System security solution(H/w and S/w),**"

2. Further, I hereby certify that

   I have read the provisions of the all clauses and confirm that notwithstanding anything stated elsewhere to the contrary, the stipulation of all clauses of Tender are acceptable to me and I have not taken any deviation to any clause.

3. I further confirm that any deviation to any clause of Tender found anywhere in my Bid, shall stand unconditionally withdrawn, without any cost implication whatsoever to the REC PDCL.

4. Our bid shall remain valid for period of 180 days from the last date of bid submission.

Date:
Place:

Signature……
Full Name……
Designation……
Address……

Note: In absence of above declaration/certification, the Bid is liable to be rejected and shall not be taken into account for evaluation.

Form-II

System security solution (H/w and S/w),

PRE QUALIFICATION CRITERIA DETAILS

1. THE FIRM

2. Name _____

Regd. Address _____

a) Address of Office _____

b) Contact Person's

i) Name & Design. _____

ii) Address _____

iii) Tel No. Landline_____**Mobile** _____

iv) Email ID _____

3. Type of Firm: **Private Ltd./ Public Ltd./ Cooperative/**
(Please tick) **Partnership/ Proprietor**

4. PAN _____

5. Service Tax Reg. No.:

6. E.M.D. Details **Rs._**
BG/DD No._
Name & Address of Bank

Please upload duly signed copies by authorized signatory of documentary evidence e.g. work order, corresponding satisfactory job completion certificates from clients with amount of work order in support of above and any other document indicated in prequalifying criteria)

Signature……
Full Name……
Designation……
Address……..

Form-III

Financial Bid **PROFORMA OF SCHEDULE OF RATES**

Bidder Name:

Tender: Supply and installation of IT Security Solution (Hardware and Software)

S.No	Type of Resource	Nos.	Rate (per Unit)	Applicable taxes	Total all inclusive unit price	Total Amount
1	IT System Security Solution with 3 year warranty support	1				
2	AMC for 4th year as per SLA	1				
3	AMC for 5th year as per SLA	1				
Total All Inclusive Value (Rs.)						

Bidders are to quote their rates strictly as per above format.

The rates are invited for entering into a rate contract valid for 1.5 years.

Prices are to be quoted accordingly. RECPDL reserves the right to increase the RC quantity (on same rate and terms & conditions) by another 20% if required.

*The quantities mentioned above are indicative and for bid evaluation purpose. Actual quantity may vary as per the site requirement and the Release orders will be placed accordingly.

FORM IV

FORMAT FOR NO-DEVIATION CERTIFICATE

Unless <u>specifically</u> mentioned in this schedule, the tender shall be deemed to confirm the RECPDCL's specifications:

S. No.	Clause No.	Details of deviation with justifications

By signing this document we hereby withdraw all the deviations whatsoever taken anywhere in this bid document and comply to all the terms and conditions, technical specifications, scope of work etc. as mentioned in the standard document except those as mentioned above.

Seal of the Company:

Signature

Name

Note: In absence of above declaration/certification, the Bid is liable to be rejected and shall not be taken into account for evaluation.

FORM-V

MANUFACTURER AUTHORIZATION FORM

(To be submitted on OEM's Letter Head)

Date: …….

ICB No.: …….

Invitation for Bid No.: ……..

Alternative No.: …….

To,

The Nodal Officer (R-APDRP Part-A Project)

Govt. of Goa, Electricity Department

Panjim, Goa 403001

Sir,

WHEREAS M/s. *[name of OEM]*, who are official manufacturers of …… having factories at *[address of OEM]* do hereby authorize M/s *[name of bidder]* to submit a Bid in relation to the Invitation for Bids indicated above, the purpose of which is to provide the following Goods, manufactured by us

…….

and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty in accordance with Clause 26 of the General Conditions of Contract or as mentioned elsewhere in the Tender Document, with respect to the Goods offered by the above firm in reply to this Invitation for Bids.

We hereby confirm that in case, the channel partner fails to provide the necessary services as per the Tender Document referred above, M/s *[name of OEM]* shall provide standard warranty on the machines supplied against the contract. The warranty period and inclusion / exclusion of parts in the warranty shall remain same as defined in the contract issued to their channel partner against this tender enquiry.

Yours Sincerely,

For ……..

Authorized Signatory

Note: In absence of above declaration/certification, the Bid is liable to be rejected and shall not be taken into account for evaluation.

REC Power Distribution Company Limited

ANNEXURE-A
PERFORMANCE BANK GUARANTEE

M/s. REC Power Distribution Company Ltd.
1016-23, 10th Floor, Devika Tower,
Nehru Place,
New Delhi

(With due Rs.100/- stamp duty, if applicable)

OUR LETTER OF GUARANTEE No. : ……..... **Date: ……..**

Amount: ……. **Valid Date: ……**

Bank Name & Address: ……

In consideration of REC Power Distribution Company Ltd. having its office at 1016-1023, 10th floor, Devika Towers, Nehru Place, New Delhi (hereinafter referred to as "RECPDCL" which expression shall unless repugnant to the content or meaning there of include all its successors, administrators and executors) and having entered into an agreement dated _____/issued Work Order No._____ dated _____with/on as_____ (hereinafter referred to as "The Courier service" which expression unless repugnant to the content or meaning thereof, shall include all the successors, Administrators and executors).

WHEREAS the Agency/Franchisee having unequivocally accepted to supply the materials as per terms and conditions given in the Agreement accepted to providing courier service as per terms and conditions given in the Agreement dated _____ /Work Order No. _____ dated _____ and RECPDCL having agreed that the Agency/Franchisee shall furnish to RECPDCL a Performance Guarantee for the faithful performance of the entire contract, to the extent of 10% (ten percent) (or the percentage as per the individual case) of the value of the Work Order i.e. for _____.

We, _____ (The Bank) which shall include OUR successors, administrators and executors herewith establish an irrevocable Letter of Guarantee No. _____ in your favour for account of _____ (The Agency/Franchisee) in cover of performance guarantee in accordance with the terms and conditions of the Agreement/work Order.

Hereby, we undertake to pay upto but not exceeding _____ (say _____ only) upon receipt by us of your first written demand accompanied by your declaration stating that the amount Claimed is due by reason of the Agency/Franchisee having failed to perform the Agreement and despite any contestation on the part of above named Agency/Franchisee.

This Letter of Guarantee will expire on _____ including 30 days of claim period and any claims made hereunder must be received by us on or before expiry date after which date this Letter of Guarantee will become of no effect whatsoever whether returned to us or not.

_____
Authorized Signature
Chief Manager/Manger

Seal of Bank

Annexure B

ACCEPTANCE FORM FOR PARTICIPATION IN REVERSE AUCTION EVENT

(To be signed and stamped by the bidder)

In a bid to make our entire procurement process more fair and transparent, RECPDCL intends to use the reverse auctions as an integral part of the entire tendering process. All the bidders who are found as technically qualified based on the tender requirements shall be eligible to participate in the reverse auction event.

The following terms and conditions are accepted by the bidder on participation in the bid event:

1. RECPDCL shall provide the user id and password to the authorized representative of the bidder. *(Authorization Letter in lieu of the same shall be submitted along with the signed and stamped Acceptance Form).*
2. RECPDCL decision to award the work would be final and binding on the supplier.
3. The bidder agrees to non-disclosure of trade information regarding the purchase, identity of RECPDCL, bid process, bid technology, bid documentation and bid details to any other party.
4. The bidder is advised to fully make aware themselves of auto bid process and ensure their participation in the event of reverse auction and failing to which RECPDCL will not be liable in any way.
5. In case of bidding through Internet medium, bidders are further advised to ensure availability of the infrastructure as required at their end to participate in the auction event. Inability to bid due to telephone line glitch, internet response issues, software or hardware hangs, power failure or any other reason shall not be the responsibility of RECPDCL.
6. In case of intranet medium, RECPDCL shall provide the infrastructure to bidders. Further, RECPDCL has sole discretion to extend or restart the auction event in case of any glitches in infrastructure observed which has restricted the bidders to submit the bids to ensure fair & transparent competitive bidding. In case an auction event is restarted, the best bid as already available in the system shall become the basis for determining start price of the new auction.
7. In case the bidder fails to participate in the auction event due any reason whatsoever, it shall be presumed that the bidder has no further discounts to offer and the initial bid as submitted by the bidder as a part of the tender shall be considered as the bidder's final no regret offer. Any offline price bids received from a bidder in lieu of non-participation in the auction event shall be out rightly rejected by RECPDCL.
8. The bidder shall be prepared with competitive price quotes on the day of the bidding event.
9. The prices as quoted by the bidder during the auction event shall be inclusive of all the applicable taxes, duties and levies and shall be FOR at site.
10. The prices submitted by a bidder during the auction event shall be binding on the bidder.
11. No requests for time extension of the auction event shall be considered by RECPDCL.
12. The original price bids of the bidders shall be reduced on pro-rata basis against each line item based on the final all inclusive prices offered during conclusion of the auction event for arriving at Contract amount.

Signature & Seal of the Bidder