Kamarajar Port Limited

(erstwhile Ennore Port Limited)

Expression of Interest

Cyber Security Audit

#17, Jawahar Building, Rajaji Salai, Chennai-600001
e-mail: krishsam@kplmail.in || Ph: 044 - 25251666

Expression of Interest

KPL would like to engage a third party firm to perform services including a cyber security audit, review of their existing IT policies, creation of IT policies in line with ISO 27001 and ISMS readiness. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis of the following with respect to CERT-IN guidelines:

- Current IT infrastructure of KPL
- Network and devices in use
- Operating systems and databases at Server level and User level
- Application packages and databases
- IT Policies including Operational Procedures in the current IT setup at KPL
- Identification of vulnerabilities, security flaws, gaps and loopholes
- Carry out ethical Internal and External Penetration Test for KPL IT setup and network

To this EOI document, a draft Request For Proposal (RFP) for the above mentioned work is enclosed for the ready reference of the prospective Bidders.

KPL is inviting comments on the 'Scope of Work', 'Eligibility Criteria', 'Deliverables' including 'Budgetary Offer' only from the CERT-IN empanelled Agency.

Based on the responses received KPL may alter the draft RFP and may also initiate separate action for inviting proposals from the CERT-IN empaneled Agency through open tender.

Time line for submission of Expression of Interest by the CERT-IN empaneled Agency is as below:

S.No.	Planned activity	Proposed timelines
1.	Issue of EoI to the bidders	31 Aug 2017
2.	Last date for submission of written queries by interested bidders for clarification on RFP	5 Sep2017
3.	KPL response to the queries	9 Sep2017
4.	Last date for submission of response to EOI	12 Sep2017

The Response to this EoI may be sent by Post to the following Address before **12th September 2017**:

The General Manager
Kamarajar Port Limited
#17, Jawahar Building,
Rajaji Salai, Chennai-600001
e-mail: krishsam@kplmail.in

General Manager (Operations)
Kamarajar Port Limited

- DRAFT -
Request for Proposal

KPL/IT/ITS/2017 **dd-mm-2017**

1 Background and Objective of the Assignment

KPL would like to engage a third party firm to perform services including a cyber security audit, review of their existing IT policies, creation of IT policies in line with ISO 27001 and ISMS readiness. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis of the following with respect to CERT-IN guidelines:

- Current IT infrastructure of KPL
- Network and devices in use
- Operating systems and databases at Server level and User level
- Application packages and databases
- IT Policies including Operational Procedures in the current IT setup at KPL
- Identification of vulnerabilities, security flaws, gaps and loopholes
- Carry out ethical Internal and External Penetration Test for KPL IT setup and network

KPL would like to have the audit performed in a phased manner, wherein the

a. The **First Cyber Security Audit** exercise needs to be commenced within 10 business days of issuing the Work Order. This needs to be done at all offices Locations (KPL Registered Office and KPL Port Offices) and Departmental end users for all types of IT systems of KPL for Cyber Security. Report of Cyber Security Gaps along with the recommendations needs to be provided by the Bidder and based on the same security Gap analysis and action would be taken at KPL end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 business days of commencement. Creation of Policies, etc need to be completed within next 10 business days.
b. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, KPL would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by KPL has been completed, the bidder would be informed accordingly by concerned KPL representative, and thereafter the bidder should commence the Second Phase of Cyber Security Audit exercise. The time taken by KPL for bridging the Cyber Security Gap will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same.
c. The **Second Cyber Security** Audit needs to be completed within 20 business days after concerned KPL representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to review and ensure that remediation action has been taken against all the observation points/gaps. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current Cyber Security status of KPL.

2 Eligibility Criteria

2.1 The bidder should be empanelled Information Security Auditors on Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information

Technology Ministry of Communications and Information Technology, Government of India as on 31.08.2017.

2.2 The bidder must have provided services of IT Security Audit for at least last three (3) financial years as on 31.03.2017

2.3 The bidder must possess CISA/ CISSP/ ISO 27001 certification in the field of IT Security Audit.

2.4 The bidder must have done IT Security Audit for at least 3 (three) large scale, enterprise-level organisation and at least 2 (two) PSUs/Govt.

2.5 The bidder shall be financially sound i.e., it must have made profits in the immediately preceding three financial years (i.e. FY 16-17, FY 15-16 and FY 14-15).

2.6 The bidder must have a GSTIN Number, certificate of incorporation and PAN Number.

Documentary evidence in respect of above pre-qualification parameters must be attached or else bids will liable to rejected.

3 Scope of Work:

The Scope of work for Cyber Security Audit would be as per the Guidelines of CERT-IN and would be under the following broad categories:

3.1 Cyber security audit including the following:

a. Evaluation and Gap analysis of the Current IT infrastructure of KPL
b. Review of Software Applications and Packages that are exposed to Internet in KPL such as Online Pass System, GIS based Land Management System, RFID based Port Access System, Antivirus Software, etc.
c. Review of Operating Systems and System Software such as Server Software, Domain controller Server, Server Hardware such as Blade Servers, Rack Servers, etc.
d. Review of Network architecture including connections of leased lines between Corporate and Port Office. Routers & Firewalls in KPL.
e. Controls of Internet and other network access to various end-users by firewalls and anti-virus policies.
f. Review of business justification of firewall rules and open ports
g. Segmentation of network
h. Review of Network Security monitoring process and segregation of duties (SoD) in network management
i. Identification of vulnerabilities, security flaws, gaps and loopholes
j. Carry out ethical Internal and External Penetration Test for KPL IT setup and network.
k. Analyze all reports, logs, etc. of the cyber security devices installed in KPL and provide input on cyber security policies for the same.

3.2 Review of the current IT Security Policy, Creation of IT Policies as per ISMS guidelines (which are not there at KPL; and required as per ISMS)and provide recommendations for a roadmap to quality standard ISO 27001, including suggestions for best practices and procedures for KPL

3.3 Documentation of Cyber Crisis Management Plan (CCMP) for KPL IT Facilities which will contain strategy followed in case of a Cyber-attack or threat in KPL. The CCPM will encompass all units of KPL as the cyber-attack may happen at any branch location of KPL

4 Technical terms:

The bidder should provide the following details along with documentary proof:

S.No	DESCRIPTION	REPLY	REMARKS / DOCUMENTS ATTACHED, IF ANY
1.	Number of years the bidder has been undertaking IT Security Audit (Attach necessary documentary proof e.g. Work Order / Completion certificate .)		
2.	Details of Authorized Contact Person 1. Name, 2. Designation, 3. Telephone. No. with STD code, 4. Mobile No. 5. E-mail ID		
3.	City-wise details of offices in India with contact number -In Chennai -Outside Chennai List to be enclosed		
4.	Project Activity offerings vis-à-vis Scope – Brief write up indicating 1. Methodology, 2. Standards, 3. **Licensed automated tools etc. to be adopted** Please specify the tools and its features that will be used		
5.	Name, Designation and Qualification of the Personnel to be deployed for IT Security Audit. Number of Project accomplished successfully and number of project(s) on which they are working		
6.	International Security standards to be followed in relation to the deliverables.		
7.	Certification, if any, awarded in the field of Security Audit like CISA, ISO 27001, CISSP & ethical hacking certified.		
8.	Testimonials & Recommendation Letters **(Attach necessary documentary proofs.)**		
9.	Is the bidder having good understanding of ISO 27001 – Yes/No? (**(Attach necessary documentary proofs.)**)		

5 Please provide details of at least Three (3) large scales, enterprise-level projects with min Two (2) PSUs executed by your organization in similar nature of work. (Attach necessary documentary proofs.)

S. No.	Client Name and Address, Contact Person & Tel. No.	Project start and end dates	Project scope	Audit Tools Used	Security Standard Used
1					
2					
3					
4					
5					

6 Commercial Terms:

PROJECT RESOURCES & FEES

6.1 Project Team Size:

The person deployed should have suitable auditor qualification and certifications such as CISA / CISSP / ISO 27001 Assessor/ISA or any other formal security auditor qualifications etc.

6.2 Fees (in INR):

S. No.	Services Offered	Total Charges (in Rs.) (inclusive of Taxes)
1	First Phase of the Cyber Security Audit, Submission of Report & Policies, etc	
2	Second Cyber Security Audit	
3	Total	

Please Note while quoting-

- The rates quoted above should be inclusive of all expenses including out of pocket expenses, travel, boarding lodging etc. at the respective locations. If there are any other charges quoted separately the bid will not be considered and may be disqualified.
- Taxes and Levies to be specified clearly in Rs. term.

6.3 Payment Terms:

- 100% of the "First Phase of the Cyber Security Audit, Submission of Report & Policies, etc" on completion/submission and acceptance of Report by KPL Management.
- 100% of the "Second Cyber Security Audit" on completion/submission and acceptance of Report by KPL Management.

7 Deliverables of the Engagement - Reports and Schedule of Deliverables

7.1 Reports

Third Party Audit Firm will produce a report which should include the overall cybersecurity protection status considering people, process and technology. The cybersecurity assessment report/audit report should include expert recommendations which will make the KPL It environment secure and sustainable. Report should include the following sections but not limited to:

1) Assessment report on the Information/IT Security Policy of KPL and provide recommendations for a roadmap to quality standard ISO 27001, including suggestions for best practices and procedures for KPL

2) Development of the Information Security/IT related Policies, as per ISMS which should include:
    - Access control
    - Asset management
    - Change Management
    - Backup and Recovery
    - IT System Operations security
    - Network and Communications security
    - System acquisition, development and maintenance
    - IT Risk Management
    - Information security incident management
    - Information security aspects of business continuity management (BCM)
    - Information and information related devices disposal policy
    - Compliance and Regulatory requirements management
    - Physical and environmental security

3) Cyber Security Audit Report (along with recommendations) on KPL's IT environment, as per CERT IN guidelines which should include but not limited to:
    - Access Control
    - Network Security Management
    - Database Management Process
    - Backup & Restore Policy and Backup Plan
    - Log management and monitoring policies for database, applications, router, firewall and operating systems
    - Incident Management and resolution process of the incidents
    - Patch update, bug fix and anti-Virus update process within KPL
    - Report on Penetration Testing and Vulnerability scan

4) Drafting the Cyber Crisis Management Plan (CCMP) for KPL IT Facilities

7.2 Schedule of Deliverables

The duration of the assignment is about **50 Business days** *excluding* the time required for KPL to bridge the gaps as much as possible based on the finding of the **First Cyber Security Audit** exercise.

Deliverable	**Tentative Duration / Periodicity**
• Inception report including outline of cyber security and ISO 27001 requirements, audit Plan, Reporting Formats, work plan, documentation formats, dates and location of proposed cyber audit exercise	1 week
• Weekly Status Reports showing proposed vs actual progress, delays (if any), and support required, gaps identified till date etc..	Every Week
• Summary of Cyber Audit findings, including identification tests and the results of the tests need to be shared with concerned KPL officials on a weekly basis and as and when required by KPL.	Weekly/ As & when requested

Deliverable	Tentative Duration / Periodicity
Prepare and submit a (i) draft Cyber security and IT audit report, (ii) draft Information/IT Security related policies (iii) Cyber Crisis Management Plan (CCMP) for KPL IT Facilities, and (iv) Expert Recommendations on the identified gaps . The audit report will have the following elements included in it: • Development of the Information Security/IT related Policies, which should include: ○ Access control ○ Asset management ○ Change Management ○ Backup and Recovery ○ IT System Operations security ○ Network and Communications security ○ System acquisition, development and maintenance ○ IT Risk management ○ Information security incident management ○ Information security aspects of business continuity management (BCM) ○ Information and information related devices disposal policy ○ Compliance and Regulatory requirements management ○ Physical and environmental security • Assessment Report (along with recommendations) on KPL's IT environment which should include but not limited to: ○ Access Control ○ Network Security Management ○ Database Management Process ○ Backup & Restore Policy and Backup Plan ○ Log management and monitoring policies for database, applications, router, firewall and operating systems ○ Incident Management and resolution process of the incidents ○ Patch update, bug fix and anti-Virus update process within KPL ○ Report on Penetration Testing and Vulnerability scan • Document Cyber Crisis Management Plan (CCMP) for KPL IT Facilities which will contain strategy followed in case of a Cyber-attack or threat in KPL. The CCPM will encompass all units of KPL as the cyber-attack may happen at any branch location of KPL	5 weeks
• Share the reports and findings with KPL and relevant stakeholders only. • Presentations on the Cyber Security Audit Report, its findings, conclusions, and recommendations for Gap Analysis and Plugging, as per CERT-In guidelines, need to be made to the management of KPL as required. Recommendations should also be given for Quality Standard ISO 27001, as this is also a prime objective of the Cyber Security Audit Output.	1 week
• Submission of final reports with required guidelines and documents	1 week

8 Audit Approach and Audit Considerations:

The independent Cyber security audit will be undertaken through an evaluation of risk management by assessing total chain process of IT environment for operation integrity and operational management.

The Consultant shall sign a Confidentiality Agreement before starting the assignment, which will ensure the confidentiality and integrity of the content, data, applications, logics, structure, designs and other property of the Client, which should be shared, given access, and will be used by the Consultant during the execution of the assignment.

The Consultant should take care of the following considerations and details at the beginning of the Cyber Security Audit exercise:

1. Approach and Methodology in which the Cyber Security Audit activity is to be done, this will include the time frame of each activity so as to organize the cyber audit activity for better control and monitoring.
2. Standards of Security and Quality that are to be followed during the Cyber Security Audit activity.
3. Tools and Software that may be used for the cyber security audit activity. All tools and software used by the bidder need to be licensed.
4. Any Additional and Mandatory standards of Cyber Audit regulation as required for CERT-IN Audit, should be made available and applicable by the Auditor.
5. All the cyber security reports, device logs, etc. have to be shared with CERT-IN office representatives by the bidder. The purpose of the same is to keep CERT-IN informed about the perceived and possible cyber threat to KPL at present and in future.

9 Instructions and Timelines for Responding

Instructions for Responding:

1. Any questions and/or requests for clarification relating to this RFP (Technical) should be sent to **The General Manager (Operations), KPL** at krishsam@kplmail.in by **dd-mm-2017**. KPL expects to respond to all questions by **dd-mm-2017.**
2. Responses to the RFP must be sent to **The General Manager (Operations), KPL** by **dd-mm-2017** in the NIC's e-procurement portal.
3. Please identify a lead contact within your organization for the purpose of this RFP and include all relevant contact details (e-mail address, phone number and office address) within your response.
4. KPL intends to make a decision by **dd-mm-2017**.

Important dates:

S.No.	Planned activity	Proposed timelines
1.	Issue of RFP to the bidders	
2.	Last date for submission of written queries by interested bidders for clarification on RFP	
3.	KPL response to the queries	
4.	Last date for submission of response to RFP	
5.	Evaluation of response (including presentation of the response by bidder (if required))	
6.	Award of contract	

10 Other Terms & Conditions

Period of validity of quotation:

The bidder shall hold their quotations valid for 60 (sixty) days from the date of opening of quotation. In exceptional circumstances, prior to the expiry of the original quotation validity period, KPL may request the Company/Firm for a specified extension of the period of quotation validity. The request and the response thereto shall be made in writing and will be binding on both the parties.

Earnest Money Deposit:

An Earnest Money Deposit of Rs. _____/- (Rupees _____ only) in form of a crossed banker's cheque, Bank Draft favouring "Kamarajar Port Limited" drawn on any Scheduled Bank payable at Chennai be accompanied with the offer; failing which the offer will not be considered. The said earnest money deposit will be refunded to unsuccessful bidders. Also the said earnest money deposit will be refunded to successful bidder after confirmation of Performance Guarantee. Earnest Money to be deposited along with the Technical bid. **'The quotation furnished without EMD amount would be rejected.**

Performance Guarantee (PG):

1 The successful Bidder, at its own expense, shall submit a Performance Guarantee within 20 Business days of the date of notice of the award of the Contract. A Performance Bank Guarantee, payable on demand in terms of **Annexure-II**, for an amount calculates at the rate of ten percent (10%) of the contract value.

2 Performance Bank Guarantee must be irrevocable and drawn on a Scheduled Bank in favour of Kamarajar Port Limited, payable at Chennai.

3 Failure of the successful Bidder to comply with the above requirements shall constitute a sufficient ground for the annulment of the award and forfeiture of the EMD.

4 The Performance Bank Guarantee may be discharged / returned by KPL after the completion of the Contract upon being satisfied that successful Bidder has successfully performed its obligations under the Contract. The Performance Bank Guarantee shall be valid for the entire duration of the Contract period plus three months thereafter as a claim period.

5 in the event the successful Bidder being unable to perform its obligations under the Contract, during the Contract period, for whatsoever reason, the Performance Bank Guarantee would be encashed by KPL.

Others:

1. The bidder shall designate the official mailing address and place to which all correspondence shall be forwarded by KPL.
2. The quotation shall be submitted in two parts, **Technical and Commercial.**
3. Last date for submission of tender is **dd.mm.2017 1500 Hrs IST**. The tenders will be opened on **dd.mm.2017 1530 Hrs IST.**
4. The Bids should be submitted in the NIC's e-procurement Portal in the corresponding section Technical and Commercial.

During evaluation of bids, KPL may, at its discretion, ask the bidder for clarification of its bids. Also KPL reserves the right to accept or reject any bid, and to annul the tendering process and reject all bids, at any time prior to the award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected Company/Firm or Company/Firms on the grounds for KPL's action.

Force Majeure:
If at any time during the existence of this contract either party is unable to perform in whole or in part any obligations under this contract because of war, hostility, military operations, civil commotion, sabotage, quarantine, restrictions, acts of God and acts of Government (including but not restricted to prohibitions of export and import), fires, floods, explosions, epidemics, strikes, or any other labour trouble embargoes, then the date of fulfillment of any obligations engagement shall be postponed during the time when such circumstances are operative. Any waiver/extension of time in respect of the delivery of any installment or part of the goods shall not be deemed to be waiver/extension of time in respect of the remaining deliveries.

If operation of such circumstances exceed three months, either party will have the right to refuse further performance of the contract in which case neither party shall have the right to claim eventual damage.

Arbitration:
All disputes or difference whatsoever arising between the parties out of or relating to the construction, meaning and operation or effect of this contract or the breach thereof shall be settled by reference to arbitration by a sole arbitrator to be nominated by the Chairman & Managing Director (CMD) of Kamarajar Port Limited. The award made in pursuance thereof shall be binding on both parties. The provisions of Arbitration and Conciliation Act 1996 shall apply to this arbitration.

The venue of arbitration shall be Chennai.

Termination for Default
KPL may, without prejudice to any other remedy for breach of work order, by written notice of default, sent to the Bidder, terminate this work order in whole or in part.
If the Bidder fails to deliver any or all of the services within the time period(s) specified in the work order, or any extension thereof granted by KPL.
If the Bidder fails to perform any other obligation(s) under the work order; and If the KPL, in either of the above circumstances, does not remedy his failure within a period of 7 days (or such longer period as KPL may authorize in writing) after receipt of the default notice from KPL.

CONFIDENTIALITY
All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner whatsoever to any third party, except with KPL's written permission. In this regard bidder has to enter into Non Disclosure Agreement with KPL as per Annexure- I.

SET OFF
Any sum of money due and payable to the Bidder (including security deposit refundable to him) under this contract may be appropriated by KPL or any other person or persons contracting through KPL and set off the same against any claim of KPL or such other person or persons for payment of a sum of money arising out of this contract or under any other contract made by the Bidder with KPL or such other person or persons contracting through purchaser.

MERGER & ACQUISITIONS
In case of mergers and acquisitions of Bidder Company, all contractual conditions and obligations shall automatically get transferred to acquiring company/entity and acquiring company must assume all the obligations of the contract till the end of the contract period.