RFT for Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food supplies and Consumer Welfare, Govt. of Odisha

E-Tender No. 242/29(13)/2037/STPI-BH/2021

Date: 29.11.2021

Last Date for Submission of bids: 20th of November, 2021at 3.00 PM

Opening of Technical Bids: 21st of November, 2021at 3.00 PM

ENVISAGED BY

Department of Food supplies and Consumer Welfare

Govt. of Odisha

SOFTWARE TECHNOLOGY PARKS OF INDIA

(Ministry of Electronics & I.T. (MeitY), Govt. of India)

STPI ELITE Tower, Plot No. 2/A, IDCO Industrial Area, Gothapatna

Post-Malipada, District-Khurda, Bhubaneswar-751003

Table of Contents

1. Invitation for Bids

Software Technology Parks of India (STPI), Bhubaneswar invites **"RFT for Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food supplies and Consumer Welfare, Govt. of Odisha"** in Two-Bid System**.** This RFT document is being published on web portal https://bhubaneswar.stpi.in and https://eprocure.gov.in/eprocure/app. Eligible bidders are requested to download the document and submit the bids online in CPP Portal. A copy of technical bid only is required to submit in a sealed envelope on or before 20.12.2021, 15:00 during working hours. Interested bidders are expected to examine the tender document carefully. Failure to furnish all information required as per the Tender Document may result in the rejection of the Bid. No bid will be accepted after the above mentioned date and time. STPI will not be responsible for any postal delay. Tenders received late or without EMD will be rejected automatically. Any subsequent corrigendum/ clarification will be made available on the website. Details may be downloaded from our website https://bhubaneswar.stpi.in.

Publishing date	29.11.2021, 16:00
Seek clarification start date	29.11.2021, 16:00
Seek clarification end date	06.12.2021, 16:00
Bid submission start date	29.11.2021, 16:00
Bid submission end date	20.12.2021, 15:00
Technical bid opening date	21.12.2021, 15:00
Financial bid opening date	Will be notified later only to the technically qualified bidder
Address of sending proposal	The Director, Software Technology Parks of India Plot 2/A, IDCO Industrial Area, Gothapatna, PO: Malipada Bhubaneswar-751003
Mode of Submission	Online
Bid Processing Fee	Rs. 10,000/- + GST@18% through digital payment

	mode like NEFT/RTGS/BHIM.
Earnest Money Deposit (EMD)	Rs. 10,00,000/- (Rupees Ten Lakhs only) in the form of Demand Draft / Bank Guarantee from a scheduled commercial bank in favor of STPI, Bhubaneswar or through digital payment mode like NEFT/RTGS/BHIM.
Bid Validity Period	One Hundred Eighty (180) Days from the date of submission of Technical Bid

Yours Sincerely

Director

Software Technology Parks of India

Plot 2/A, IDCO Industrial Area,

Gothapatna, PO: Malipada

Bhubaneswar-751003

Website: bhubaneswar.stpi.in

2. Introduction

2.1. Department of Food Supplies and Consumer Welfare

Food, Supplies and Consumer Welfare Department is a composite Department with the status of both Secretariat and Directorate. Hon'ble Minister, F.S. & C.W. is Minister In-Charge of the Department. Commissioner-Cum-Secretary to Government is Secretary In-Charge of the Department. Secretary of the Department also functions as the Director, Food Supplies and Controller of Supplies.

Government of Odisha has undertaken the practice under FSCW Department who is looking after the Targeted Public Distribution System and Procures paddy from the farmers at the minimum support price. Department holds the responsibility for distributing the same to the consumers through the established network of Fair Price Shops (FPSs).

India's Public Distribution System (PDS) is one of the world's largest food security schemes. The PDS was created to improve the targeting of subsidies to people that most needed them. PDS is operated under the joint responsibility of Central Government and State Governments/Union Territory (UT) Administrations.

For the state of Odisha, the ceiling stands at 82% of the rural population and 56% of the urban population, 78% of the entire state population covered under AAY (Antyodaya Anna Yojana) and PHH (Priority Households). Odisha is the 11th most populous state in India with a population of 41,947,358 (according to the 2011 Census). PDS in Odisha is spread over 12,500 FPS in 314 Blocks and 109 Urban Locations in 30 districts.

2.2. Software Technology Parks of India (STPI)

2.2.1. Brief Profile

Software Technology Parks of India (STPI), an organization under the Ministry of Electronics and Information Technology, Government of India has been set up with distinct focus for promotion of software and IT exports from the Country. Since its inspection in 1991, STPI has come a long way and become highly successful in its mission as catalyst in positioning India as the most preferred destination for outsourced IT and IT enabled services, a fact, aptly proven by the stupendous growth in IT exports. STPI units represent more than 90% share of National Software Exports. The above statistics reveal that Govt. of India's vision of making India as IT super power has been very successful through STPI.

The concept of Software technology Park has emanated from the need to provide infrastructure facilities such as High Speed Data communication services, built up space and Hi-tech incubation facilities to nucleate growth of software exports. In fact, STPI have revolutionized the concept of cooperative competitiveness of the infrastructure facilities and capital equipment's by the Software units in optimal, effective and efficient

manner at an affordable cost. The concept has greatly helped young entrepreneurs and Small & Medium Enterprises (SMEs) to kick start their operation with no waiting time and absolve them for making investments in creating captive infrastructure.

At present STPI has more than 60 centres across the country including Bhubaneswar, Rourkela, Berhampur in the State of Odisha while a fourth centre is being set up in Balasore. The Bhubaneswar Centre of STPI is one of the premier centres established along with Bangalore and Pune in the year 1991.

3. Instruction to Bidders

3.1. Definitions

a) "STPI" means the "Software Technology Parks of India" that has invited the bids for selection of Bidder/ System Integrator (SI) and with which the selected SI signs the Contract for the Services and to which the selected SI shall supply the necessary hardware and provide services as per the terms and conditions of the RFT.

b) "SI" means "System Integrator" - any entity or person or association of persons who is eligible to submit proposals to provide services to the STPI under this Contract.

c) "Contract" means the Contract signed between the SI and the STPI.

d) "Project specific information" means such part of the Instructions to Bidders used to reflect specific project and assignment conditions.

e) "Day" means calendar day.

f) "Government" means the Government of Odisha unless otherwise specified

g) "Instructions to Bidders" means the document, which provides the bidders with all information needed to prepare their proposals.

h) "Proposal" means the Technical Proposal and the Financial Proposal.

i) "RFT" means the Request for Proposal prepared by the STPI for the selection of SI.

j) "Assignment / job" means the work to be performed by the SI pursuant to the Contract.

k) "Sub-agencies" means any person or entity to which the SI subcontracts any part of the Assignment/job.

3.2. Introduction

a) The STPI will select a Bidder (SI) in accordance with the method of selection specified in the Proposal Evaluation Section.

b) The name of the assignment is in the Data Sheet. Detailed scope of the assignment has been described in the Section-5.

c) The date, time and address for submission of the proposals have been mentioned in the "Invitation for Bid" section of the RFT.

d) The eligible bidders are invited to submit their Proposal, for assignment - **"Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food supplies and Consumer Welfare, Govt. of Odisha"**. The Proposal will be the basis for contract negotiations, if required, and ultimately for a Contract with the selected SI.

e) Bidders should familiarize themselves with local conditions and take them into account for preparing their Proposals.

f) The STPI will provide assistance to the Bidders including inputs and facilities specified in the Data Sheet, for obtaining licenses and permits needed to carry out the Assignment, and make available relevant project data and reports.

g) Bidders shall bear all costs associated with the preparation and submission of their proposals and contract negotiations. The STPI is not bound to accept any proposal, and reserves the right to annul the selection process at any time prior to contract award, without assigning any reason or reasons and will in no case incurring any liability to the Agencies.

3.3. Clarification and Amendment of RFT Documents

a) Bidders may request a clarification on any clause of the RFT documents up to the number of days indicated in RFT before the proposal submission date. Any request for clarification must be sent through e-mail the STPI's e-mail address indicated in the RFT. The STPI will share a virtual link for discussion to only those bidders who have responded on time. Should the STPI deem it necessary to amend the RFT as a result of a clarification, it shall do so following the procedure under Para 3.3(b) below.

b) At any time before the submission of Proposals, the STPI may amend the RFT by issuing an addendum in writing or by standard electronic means. The addendum will be binding on them. To give bidders reasonable time in which to take an amendment into account in their Proposals the STPI may, if the amendment is substantial extend the deadline for the submission of Proposals.

3.4. Language of Bid & Correspondence

The Bid will be submitted by the Bidder in English language only. All the documents relating to the Bid (including brochures) supplied by the Bidder should also be in English, and the correspondence between the Bidder & STPI will be in English language only.

3.5. Proposal

The Bidders may submit one proposal only. If a Bidder submits or participates in more than one proposal, such proposals shall be disqualified. However, this does not limit the participation of the same Sub-Bidder/ sub-contractor, including individual experts, to more than one proposal.

3.6. Proposal Validity

The "Invitation for Bids" indicates the period of validity from the date of submission of the proposals by bidders. During this period, the financial proposal shall remain unchanged. The STPI will make its best effort to award the contract within this period. However, the STPI may request for extension of the validity period of their proposals. A Bidder that does not agree has the right to refuse to extend validity of their Proposals; under such circumstance the STPI shall not consider such proposal for further evaluation.

3.7. Preparation of Proposals

a) The Proposal and all related correspondence exchanged by the Bidders and the STPI shall be in English language, unless specified otherwise.

b) In preparing their proposal, Bidders are expected to examine in detail the documents comprising the RFT. Material deficiencies in providing the information requested may result in rejection of a Proposal.

c) While preparing the Technical Proposal Bidders must give particular attention to the following:

   - If a short-listed Bidder considers that it may enhance its expertise for the assignment/job by associating with other Bidder in sub- bidder, it may associate with a non-short-listed Bidder.
   - While preparing the proposal, the bidder must ensure that it proposes the minimum number and type of materials and experts as sought by the STPI, failing which the proposal shall be considered as nonresponsive.

d) Depending on the nature of the assignment, agencies are required to submit a Technical Proposal (TP).

e) The Technical Proposal shall not include any financial information. A Technical Proposal containing financial information may be declared non responsive.

f) Financial Proposals: The Financial Proposal shall be prepared using the attached Standard Forms. It shall list all costs associated with the assignment/job, including (a) Hardware & COTS cost (b) Remuneration of the Resources deployed etc. The financial proposal shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

3.8. Taxes

The Bidder shall fully familiarize themselves about the applicable taxes (such as: Good & Service Taxes, income taxes, duties, fees, levies) on amounts payable by the STPI under the Contract. All such taxes must be included by the bidder in the financial proposal. However any addition in Taxes notified by Government of India time to time shall be paid separately at the time of billing as per actual.

3.9. Currency

Bidder shall express the price of their assignment/job in Indian Rupees (INR).

3.10. Bid Processing Fees

All agencies are required to pay Rs. 10,000/- + GST@18% towards Bid Processing Fees through digital payment mode like NEFT/RTGS/BHIM. The Bid Processing Fee is Non-Refundable. Please note that the Proposal, which does not include the bid processing fees, would be rejected as non-responsive.

3.11. Earnest Money Deposit (EMD) and Bid processing Fees

a) An EMD of Rs. 20,00,000/-, in the form of Bank Draft/ BG drawn in favor of the STPI (The Director, Software Technology Parks of India, Bhubaneswar, Odisha) and payable at Bhubaneswar or through digital payment mode like NEFT/RTGS/BHIM, must be submitted along with the Proposal.

Account Details for furnishing EMD is as below:

Name of the Account Holder	SOFTWARE TECHNOLOGY PARKS OF INDIA
Name of the Bank	Bank of India
Account Number	555110110003601
IFSC Code	BKID0005551
Branch Code	0005551

Software Technology Parks of India supports payments through UPI (Unified Payments Interface) and BHIM (Bharat Interface for Money). UPI ID of Software

Technology Parks of India is "stpi@upi" and QR code for UPI payments to Software Technology Parks of India is available at www.stpi.in. Using this UPI ID, anyone can transfer money to Software Technology Parks of India with any UPI based App, including BHIM.

MSE bidders should declare their UAM number on CPPP, failing which such bidders will not be able to enjoy the benefits as per Public Procurement Policy for MSEs Order 2012.

a) Proposals not accompanied by EMD shall be rejected as non-responsive.

b) No interest shall be payable by the STPI for the sum deposited as earnest money deposit.

c) The EMD of the unsuccessful bidders would be returned back within one month of signing of the contract.

d) The EMD shall be forfeited by the STPI in the following events:

- If Proposal is withdrawn during the validity period or any extension agreed by the bidder thereof.
- If the Proposal is varied or modified in a manner not acceptable to the STPI after opening of Proposal during the validity period or any extension thereof.
- If the Bidder tries to influence the evaluation process.

3.12. Performance Security

The STPI will require the SI to provide a Performance Bank Guarantee, within 15 days from the Notification of award, for a value equivalent to 5% of the quoted project cost for each year excluding taxes. The Performance Guarantee shall valid for a period of three months beyond the date of completion of all contractual obligations/tenure The Performance Guarantee shall be renewed/amended annually. The SI shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion or extension of the project duration.

In the event of the Contractual delivery period being extended by the Buyer, the Seller shall be responsible to ensure that the validity of the Performance Guarantee is also simultaneously extended/re-validated.

In case the SI fails to submit performance guarantee within the time stipulated, the STPI at its discretion may cancel the order placed on the SI without giving any notice. STPI shall invoke the performance guarantee in case the selected bidder fails to discharge their contractual obligations during the period or STPI incurs any loss due to bidder's

negligence in carrying out the project implementation as per the agreed terms & conditions.

3.13. Forfeiture of EMD /Security Deposit/Performance Guarantee

a) If the successful bidder/bidder refuse/fails to accept Purchase Order issued by STPI or the job assigned to the bidder/bidder are not done as per the scope of work/schedule of requirement, EMD/Security Deposit will be forfeited.

b) If the Bidder withdraws tender before/after finalization of the tender, EMD will be forfeited

c) If the contract is terminated by STPI due to poor supply/violation of any clause of agreement or any bad act of selected bidder, security deposit/PG will be forfeited.

d) In case of unreasonable price quoted by the bidder for disrupting the tender process EMD of such bidder will be forfeited.

3.14. Submission, Receipt, and Opening of Proposal

a) The proposal - both technical and financial proposals, shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder them. The person who signed the proposal must initial such corrections.

b) Authorized representative of the Bidder shall initial all pages of the Technical and Financial Proposals. The authorization shall be in the form of a written letter of authorization accompanying the Proposal or in any other form demonstrating that the representative has been dully authorized to sign.

c) The proposal shall be submitted in three parts in CPP portal https://eprocure.gov.in/cppp/. Part-I should contain copy of "Bid Processing Free & Earnest Money", Part-II should contain copies of documents required for "Pre-qualification"& "Technical Bid" and Part-III should contain "Financial Bid".

d) Hard copy of technical proposal shall be placed in a sealed envelope clearly marked "TECHNICAL PROPOSAL" followed by the name of the assignment/job. The envelopes containing the Technical Proposals, EMD and bid processing fees shall be placed into an outer envelope and sealed. This outer envelope shall bear the submission address, reference number and be clearly marked "DO NOT OPEN, BEFORE 20/12/2021 03:00 PM". The STPI shall not be responsible for misplacement, losing or premature opening if the outer envelope is not sealed and/or marked as stipulated. This circumstance may be reason for rejection of the entire proposal.

e) The Proposals must be sent to the address in the Data sheet and received by the STPI no later than the time and the date indicated in the RFT, or any extension to this date. Any proposal received by the STPI after the deadline for submission shall be returned unopened.

3.15. Completeness of Tender Offer

The Bidder is expected to examine all instructions, forms, terms, conditions and deliverables in the Tender Documents. Failure to furnish all information required by the tender documents or submission of a tender offer not substantially responsive in every respect to the tender documents will be at the Bidder's risk and may result in rejection of its tender offer. The tender offer is liable to be rejected outright without any intimation to the Bidder if complete information as called for in the tender document is not given therein, or if particulars asked for in the Forms / Performa in the tender are not fully furnished.

3.16. Rejection of the Bid

a) The bidder is expected to examine all instructions, formats, terms & conditions, and scope of work in the bid document. Failure to furnish complete information or false information/documents which is not substantially responsive to the bid document in all respect shall result in rejection of bid.

b) In respect of interpretation/clarification of this bid document and in respect of any matter relating to this bid document, the decision of STPI-Bhubaneswar shall be final.

c) The bidder will have to furnish the requisite document as specified in the bid document, failing which the bid is liable to be rejected.

d) No prices are to be indicated in the Professional Bid and if the prices are mentioned in the "Technical Bid" it may lead to rejection of the bid.

e) Bids not submitted as per two bid system will be summarily rejected.

f) Bids without paper cost & EMD money will be summarily rejected.

g) The bids received after specified date & time shall not be considered.

h) The bids received through Fax/-email or any other mode other than specified in the tender document shall not be considered.

3.17. Liquidity Damage

a) Delivery of services shall be made by the vendor in accordance with the time schedule specified by STPI.

b) The Vendor will strictly adhere to the time-schedule for the performance of Work. The original Delivery Period may be re-fixed by STPI without any Liquidated damages subject to Force Majeure conditions mentioned below and also on the ground/reasons of delay attributable to the Buyer / Consignee.

c) For other cases, provided the price trend is not lower, the Delivery Period may be suitably extended for which an amount equal to the Liquidated Damages for the extended period(s) for delay in the supply of the Goods/Services after the expiry of contract delivery period /re-fixed delivery period, shall be recovered from the successful bidder as mentioned hereinafter for the extended period. No increase in price on any ground after the original/re-fixed delivery date shall be admissible during such extended period(s). Nevertheless STPI shall be entitled to the benefit of any decrease in price on account of reduction in GST taking place during extended delivery period

d) In case of delay in completion the supply and installation within the implementation timelines fixed under tender for reasons attributable to the Vendor, then STPI shall levy penalty @ 0.5% per week with a maximum limit of 5% of the contract value or PBG may be forfeited. Delay beyond 10 weeks lead to cancellation of PO/WO, forfeiture of EMD and disallowing of participation in future STPI tenders.

e) Any rectification/repairing/configuration/troubleshoot during warranty period must be attended within 24 hours of receiving verbal complain from STPI, otherwise penalty for delay in service will be charged by extending warranty period (i.e. one day for 24 hours delay after completion of 24 hours from receiving the verbal complain).

f) In case of delay beyond 3 days reason adhere to vendor, then penalty @ 0.5% per week with a maximum limit of 5% of the contract value or PBG may be forfeited.

i) In case the vendor is not being adhered to the time schedule fixed under contract, STPI has the right to cancel the Contract wholly or in part without any liability to cancellation charges and procure the Goods and Services elsewhere and in a manner decided by the client. In such case the successful Bidder shall pay the difference of the cost of Goods and Services procured elsewhere and price set forth in the Contract Agreement with the successful Bidder/ Contractor.

3.18. General Terms and Conditions

a) Prices quoted by the bidders should include all local taxes, GST, duties, levies etc., till the bid validity period.

b) The bidder has to submit the OEM authorization for sale, support and service.

c) Delivery/ installation of the solution should strictly be completed within the stipulated period of delivery. Any incident during installation will be bidder’s risks.

d) Rate/Price should be clearly quoted in figures as well as in words separately in the prescribed format attached (Price Bid) with make& model. Rate/Price quoted should be inclusive of excise duty if any and taxes (GST), freight, insurance etc.

e) The quoted price shall be firm and fixed and there shall be no change. No additional charges shall be paid other than quoted price in the bid.

f) STPI reserves the right to vary the bill of quantity and the bidder shall supply at the unit price quoted in the bid and the payment shall be done based on total unit price only.

3.19. Option Clause

STPI reserves the right to place orders for additional quantity up to a maximum of 25% of the originally contracted quantity at the same rate and terms of contract within the original Delivery Period (DP) as well as Re-fixed/Extended DP subject to :there being a requirement for the item, incorporation of Option clause in the contract, there being no downward trend in price (consent of supplier is not necessary) or if there is a downward trend, the supplier agreeing to reduce the price for the enhanced quantity duly matching with the fall in prices, and if no fruitful result will accrue by floating fresh Tender or when the store is urgently required for meeting production targets. The Option clause can be exercised (if necessary more than once) provided the cumulative of the Option clause quantities exercised does not exceed the option clause quantity provided in the contract.

3.20. Cancellation by Default

STPI may without prejudice to any other remedy for breach of terms and conditions, including forfeiture of Performance Security by written notice of default sent to the company, terminate the work / task in whole or in part after sending a notice to the Bidder in this regard. If the Bidder fails to deliver or complete the job assigned in the terms and conditions within the time period (s) specified in the Tender Document and if the Bidder fails to perform any other obligations under the terms and conditions.

3.21. Blacklisting

Company/Firm blacklisted by Govt. / PSU organization are not eligible to participate in the bidding process. If at any stage of bidding process or during the currency of work order, such information comes to the knowledge of STPI, STPI shall have right to reject the bid or cancel the work order, as the case may be, without any compensation to the bidder. The bidders have to be submit an undertaking for not being black listed since last 3 years by any Govt./PSU organization.

3.22. Arbitration

All disputes, differences, claims and demands arising under this contract agreement shall be first resolved amicably by mutual consultations. If after 15 days the parties have failed to resolve their disputes or differences by such mutual consultation, then the matter may be referred to arbitration of a sole arbitrator appointed by the Director General, STPI.

The provisions of the Arbitration and Conciliation Act, 1996 shall be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to the arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modification, Rules or re-enactments thereof. Language of proceedings shall be English. Legal disputes if any shall be subject to the jurisdiction of High Court of Delhi

3.23. Confidentiality

Any information pertaining to STPI or any other bidder involved in the project, matters concerning STPI or with the bidder that comes to the knowledge of the Bidder in connection with this contract will be deemed to be confidential and the Bidder will be fully responsible for the same being kept confidential and held in trust, as also for all consequences of its concerned personnel failing to do so. The Bidder shall ensure due secrecy of information and data not intended for public distribution.

3.24. Force Majeure

On the occurrence of any unforeseen event, beyond the control of either Party, directly interfering with the delivery of Services arising during the currency of the contract, such as war, hostilities, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts, or acts of God, the affected Party shall, within a week from the commencement thereof, notify the same in writing to the other Party with reasonable evidence thereof. Unless otherwise directed by the Procuring Entity in writing, the contractor shall continue to perform its obligations under the contract as far as reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. If the force majeure condition(s) mentioned above be in force for 90 days or more at any time, either party shall have the option to terminate the contract on expiry of 90 days of commencement of such force majeure by giving 14 days' notice to the other party in writing. In case of such termination, no damages shall be claimed by either party against the other, save and except those which had occurred under any other clause of this contract before such termination.

Notwithstanding the remedial provisions contained in Liquidated damages clauses or Cancellation by Default clauses, none of the Party shall seek any such remedies or damages for the delay and/ or failure of the other Party in fulfilling its obligations under the contract if it is the result of an event of Force Majeure.

4. Tender Evaluation

STPI will prepare a list of responsive bidders, who comply with all the Terms and Conditions of the Tender. All eligible bids will be considered for further evaluation by STPI according to the Evaluation process defined in this RFT document. The decision of STPI will be final in this regard.

4.1. Pre-Qualification Criteria

Preliminary scrutiny of the bidder's eligibility will be done as per the criteria provided below. Technical Bids of only the successful pre-qualifiers will be opened for evaluation.

Sl. #	Specific Requirements	Documentary Requirement
1.	The bidder should be registered under the Indian Companies Act. The bidder must be operating in IT/ITeS Services for the last Five years as on 31st March 2020.	Valid Certificate of Incorporation/ Registration & 5 years I.T. Returns
2.	The Bidder should have valid PAN, GST registration certification.	Copies of valid PAN & GST registration certificate
3.	The bidder must have a registered/ fully operational office in Odisha or shall furnish an undertaking at the time of bid submission that the Bidder shall establish an office in Odisha within Thirty days of being declared as the successful bidder. The office shall be maintained during the entire duration of the Contract.	Valid Ownership Document/ lease agreement/ Undertaking for Establishment of Office
4.	The bidder must have an average annual turnover of minimum Rs. 40 Crores and a positive net worth for the last three financial years as of 31stMarch 2020	– Audited Balance Sheet and Profit & Loss Statements – Certification by Chartered Accountant
5.	The bidder must have valid ISO& CMMI Level3 (Published on CMMI Institute or SEI Website) or higher certificate as on date of submission of the bid.	Copy of valid Quality Certificates

Sl. #	Specific Requirements	Documentary Requirement
6.	The bidder must have successfully implemented at least one project of minimum value of Rs. 3 Crores involving supply and installation of COTS product for any Government Department/ Bidder/ PSU in India during the last five years.	Work Orders / Contract Agreement and completion certificate or Go- Live certificate to be demonstrated showcasing as supporting documents
7.	The bidder should have experience in implementing projects involving integration with 3rd party software/ Government regulatory system.	Work Orders / Contract Agreement and completion certificate or Go- Live certificate to be demonstrated showcasing as supporting documents
8.	The proposed solution should have been implemented for any Government Department/ Bidder/ PSU in India	Case Study with Project & Client Details
9.	The bidder must have at least 40 full time employees in its payroll as on date of submission of bid.	Copy of the latest EPF deposit challan showing the number of subscribers
10.	The bidder should not be under a declaration of ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government/PSU as on the date of submission of bids.	Self-Declaration by authorized bidder
11.	The Bidder should submit valid authorization from the COTS solution OEMs	Manufacturer's Authorization Form
12.	The Bidder should submit EMD as provisioned in the RFT	Required online transaction/BG drawn as instructed
13.	The Bidder should submit Tender fees as provisioned in the RFT	Required online trancation as instructed

Note: Supporting documents needs to be submitted along with the Bid Documents in regards to pre-qualification criteria.

4.2. Technical Evaluation

Technical evaluation of only successfully pre-qualified bidders shall be done as per the parameters provided below. The Bidder has to do the POC (Proof of Concept) of the proposed solution. This shall be a part of technical evaluation.

4.2.1. POC Criteria

The Bidder can demonstrate the solution with different use-cases mentioned below by setting the environment on-site or in cloud environment. The Bidder will bear all the cost of POC. The evaluation will be done on the basis of inputs from the Evaluation committee member.

Sl No.	Functionalities
FR 1	Automatically deploy sensor agents across DB environment using implementation manager. Turn sensors on/off from single console.
FR 2	Capture and report access to sensitive objects (ex: Aadhaar, PAN).
FR 3	Alert on multiple failed logons. (Alert on 3 failed logons within 5 minutes) and publish information to SYSLOG.
FR 4	Track and report on policy violations and group by exception type. Prevent users from accessing sensitive data by killing session prior to command execution or based on returned data from SQL query (if needed).
FR 5	Monitor and report on data manipulation language (DML) commands
FR 6	Capture and report on SELECT statements.
FR 7	Report on database access including logins, client IP, server IP and source program information. (Including non-DBAs).
FR 8	Perform audits on a specific user and review all commands executed over a specific time period.
FR 9	Track execution of stored procedures, including who executed a procedure, what procedure name and when.
FR 10	Track and report all failed logins.
FR 11	Show a graphical representation of database access health across sensors and collectors. And if needed of Aggregators (with a central manager view).
FR 12	Allow drill down into the actual SQL being executed by users on any of the databases being monitored.

Sl No.	Functionalities
FR 13	Report on database access via third party tools, including logins, network and source program information.
FR 14	Configure local agent settings from management interface on appliance.
FR 15	Create an audit compliance workflow for a few users allowing for comments, escalation and signoff.
FR 16	If applicable, monitor local database activity that uses Named Pipes.
FR 17	Block DDL command (DROP, i.e.) on a database to prevent accidental or malicious activity.
FR 18	Review out-of-the-box libraries of pre-defined policies, reports, alerts for various compliance initiatives.
FR 19	Discover databases with versions and path levels that are on the network.
FR 20	Classify data in databases according to pre-defined rules on GDPR, PCI, and SOX criteria.
FR 21	Capture and Report on Database Entitlements.
FR 22	Capture and report on data definition language (DDL) commands.
FR 23	Report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.
FR 24	Create custom reports, understand detail levels.
FR 25	Group objects (sensitive and financial) and activities for use in reporting. Test auto-population of groups through a query or LDAP connection.
FR 26	Alert real-time on specific execution of a SQL command (SELECT) by a specific user.
FR 27	Define an audit review process, selecting a group of three reports and send via email for review and signoff.
FR 28	Track and audit administrative commands such as GRANT, REVOKE, DBCC, BACKUP, RESTORE, KILL, as well as all activity on all administrative (and sensitive) objects.
FR 29	Review all SQL exceptions, including all failed SQL commands. Send these as reports. (Either automatically as a report card report or audit workflow).
FR 30	Capture and report on direct server (non-network) login and associated activities by any admin type role.

Sl No.	Functionalities
FR 31	Export reports to Excel for further analysis or presentation options
FR 32	Change control process – track DDL execution by DBA, database, time, SQL command, client IP, server IP.
FR 33	Configure automatic DNS lookup to translate IP addresses into more readily identifiable information (may depend on DNS server configuration).
FR 34	Perform and capture local database activity without requiring a loopback interface connection.
FR 35	Create specific rules on observed events, sending SMTP alerts when the rules are violated.
FR 36	If applicable, monitor local database activity that uses Shared Memory.
FR 37	Capture Full SQL (including values) for specific users.
FR 38	Verify database user password information is never captured.
FR 39	Selectively alias technical information for less technical audiences.
FR 40	If applicable, monitor local database activity that uses Oracle Bequeath.
FR 41	Mask and redact critical information stored on DB when accessed directly by DBA
FR 42	Use active analytics with active threat vector use case for spotting risks
FR 43	Automatically analyze installed policies for evaluating the effectiveness and performance.
FR 44	Perform User behavioral analytics highlighting working hours and off hour activity, with observations and severity.
FR 45	Highlight any anomalous activities based on observed patterns.
FR 46	Export risky user behavior to PDF or CSV files and create a review process to automatically distribute reports on a schedule.
FR 47	Review investigation and forensics dashboard to see who has done what, when with any exceptions.
FR 48	File and Folder level encryption for Linux / Unix / Windows

The PoC should include hierarchal restrictions and access of application and database.

4.2.2. Technical evaluation Criteria

Bidders securing a minimum of 60 marks in the technical evaluation along with successful POC (Proof of Concept) will only be considered for further financial bid evaluation. Bids or Tenders which don't secure the minimum specified technical score along with successful POC (Proof of Concept) will be considered technically non-responsive and hence debarred from being considered for financial evaluation.

Sl. #	Specific Requirements	Parameter	Max. Marks	Documentary Requirement
1.	The bidder must have average annual turnover of Rs. 40 Crores in last three financial years ending at 31st March 2020 Turnover of projects implemented in India shall only be considered.	– Rs. 40 to 45Crores: 3 Marks – Rs. 45to 50Crores: 4 Marks – More than Rs. 50Crores: 5 Marks	5	– Audited Balance Sheet and Profit & Loss Statements – Certification by Chartered Accountant
2.	The bidder must be operating in IT/ITeS Services for the last Five years as on 31st March 2020.	– 5 - 10 Years: 4 Marks – 10 - 15 Years: 7 Marks – > 15 years: 10 Marks	10	Valid Certificate of Incorporation/ Registration required to be submitted along with one work order show casing the year of existance
3.	The Bidder must have a registered office in Odisha and should be operational since last 5 years.	– 5 - 10 Years: 2 Marks – > 10 Years: 5 Marks	5	Valid Ownership/ lease agreement / Certificate
4.	The bidder must have valid ISO& CMMI (Published on	– ISO 9001+27001: 4	5	Copy of valid Quality

Sl. #	Specific Requirements	Parameter	Max. Marks	Documentary Requirement
	CMMI Institute or SEI Website)certificate as on 31st March 2020	Marks - ISO 9001+27001 + CMMi Level 3& above: 5 Marks		Certificates
5.	The bidder should have experience of following number of project(s) involving implementation and support services for any Department/ Bidder/ PSU in any State or Central Government of India during last 5 years as on 31/03/2020	- >= 2Cr. &< 3 Cr.: 2 marks for each project - >= 3 Cr. &< 5 Cr.: 3 Marks for each Project - More than 5 Crore: 5 marks for each project	10	Work Orders / Contract Agreement and Completion certificate or Go-Live certificate to be demonstrated showcasing as supporting documents
6.	The bidder must have successfully implemented at least one project of minimum value of Rs. 3 Crores involving supply and installation of COTS product for any Government Department/ Bidder/ PSU in India in India during the last five years.	Each project shall carry 5 marks	10	Work Orders / Contract Agreement and completion certificate or Go-Live certificate to be demonstrated showcasing as supporting documents
7.	The bidder should have experience Handling Large volume (preferably >=1 TB) of digital data	Each project shall carry 5 marks	10	Project name and Brief scope of work with Work order

Sl. #	Specific Requirements	Parameter	Max. Marks	Documentary Requirement
8.	The bidder should have experience in implementing projects involving integration with 3rd party software/ Government regulatory system.	Each project shall carry 5 marks	15	Work Orders + Ongoing or completion certificate and project details
9.	The proposed solution should be in Forrester and Kuppingercole Leader's quadrant	5 Marks	5	Copy of Forrester Wave™: Data Security Portfolio
10.	The proposed solution should have been implemented for any Government Department/ Bidder/ PSU in India	Each project shall carry 5 marks	10	Work Orders + Ongoing or completion certificate and project details
11.	Technical Proposal	– Full Compliance to Technical Specifications	5	
		– Comprehensive ness of the project plan	2	
		– Approach for Supply and Installation	3	
		– Approach for Technical Support Services	3	

Sl. #	Specific Requirements	Parameter	Max. Marks	Documentary Requirement
		– Risk Management & Mitigation Plan	2	

Note: Supporting documents needs to be submitted along with the Bid Documents in regards to technical evaluation criteria.

4.2.3. Technical Evaluation Formula

a) All the bidders who secure a Technical Score of 60 or more will be declared as technically qualified

b) The bidder with highest technical bid (H1) will be awarded 100% score

c) Technical scores of other than H1 bidders will be evaluated using the following formula

- Technical Score of a Bidder = {(Technical Bid score of the Bidder / Technical Bid Score of H1) X 70} %

  (Adjusted up to two decimal places)

d) The Commercial bids of only the technically qualified Bidders will be opened for further processing.

4.3. Financial bid Evaluation

a) The Financial Bids of the technically qualified bidders (those who have secured equal or more than 60 of mark in technical evaluation) will be opened on the prescribed date in the presence of bidders' representatives

b) The bid with lowest Financial (L1) i.e. "lowest price quoted" will be awarded 100% Score

c) Financial Scores for other than L1 Bidders will be evaluated using the following formula

d) Financial Score of a Bidder = {(Financial Bid of L1/ Financial Bid of the Bidder) X 30}%

e) (Adjusted up to two decimal Places)

f) Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.

g) The bid price will be inclusive of all taxes and levies and shall be in Indian Rupees.

h) Any conditional bid would be rejected

i) Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail".

4.4. Combined evaluation of Technical and Financial Bids

a) The technical and financial scores secured by each bidder will be added to compute a composite Bid Score.

b) The Bidder securing Highest Composite Bid Score will be adjudicated with the Best Value Bidder for award of the project.

c) In the event the bid composite bid scores are 'tied', the bidder securing the highest technical score will be awarded the project or adopt any other method as decided by the Tendering Authority.

4.5. Award of Contract

a) After completion of the bidding process the STPI shall issue a Purchase/ Work Order to the selected Bidder, prior to the expiry of the period of Bid validity. The order will be placed in yearly basis. After completion of first year , the service will be renewed annually subjected to satisfactory performance duly certified by user department and after receipt of the necessary approval from the user department

b) The Successful Bidder shall give his acceptance within 7 days from the date of issue of PO/WO. The successful Bidder shall signed service Level Agreement with STPI.

c) The Bidder is expected to commence the assignment/job on the date and at the location specified in the RFT.

d) Liability of the successful bidder to perform the job will commence from the date of PO. The Completion Period shall be counted from the date of PO.

5. Scope of Work and Deliverables

For the modernization of Public Distribution System (PDS) including its end-to-end computerization various e-Governance initiatives have been undertaken by the Food &Civil Supplies Department. The modules are given below.

a) Complete digitization of the ration card beneficiaries

b) Computerization of Supply Chain Management

c) Automation of the FPS (Fair Price shops) by introduction of e-POS (Electronic Point of Sale)

d) Grievance Redressal system

e) Transparency Portal

f) P-PAS (Paddy Procurement Automated System)

g) Farmer Registration Module

h) Miller Application

i) DLM

Because of usage of several applications and considering the voluminous transactions of data, FS&CW Department has realized that, all transactions are conducted on the basis of the availability of data in the server, it is imperative that such data should be secured. Three major aspects of data security, Accuracy, Consistency and Confidentialities, shall be addressed through this project.

Considering the requirement of the project, STPI is appointed as consultant to Hire a competent bidder (referred as SI) to undertake the project on turnkey basis with below scope of work.

a) Procurement of the IT infrastructure as per the BOQ.

b) Installation and configuration of the Operating System, Virtual Environment and Data Encryption Tools at OSDC & STPI Elite Data Center.

c) Submission of Configuration Parameters needs and Installation Report after successful installation

d) Provide Operational support.

The licenses of the software/Subscription and warranty of hardware will be in name of "Department of Food Supplies and Consumer Welfare, Govt. of Odisha". The licenses of the software/Subscription shall be delivered digitally through e-mail.

5.1. Implementation

The COTS solution proposed by the implementing bidder shall cater to the following requirement:

5.1.1. File and Database Encryption

File and Database Encryption to be implemented to protect on premise data from theft and misuse. The solution should facilitate segregation of duties' and access on a role and rights basis. It shall limit access to sensitive data. This security mechanism should be designed to meet compliance regulations determined by the government as well as globally practice industry standards.

Encryption and decryption operations should be conducted without any consequential loss on system performance. The solution should be highly scalable for heterogeneous environments and shall facilitate the following:

a) Transparent encryption and decryption

b) Secure, centralized key and policy management

c) Granular support for regulatory compliance

d) Live data transformation

5.1.2. Data Protection for Databases

Data Protection solution for databases should provide automated sensitive data discovery and classification, real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data. It should protect against unauthorized data access by learning regular user access patterns. It should also have provision for generating real-time alerts on suspicious activities. It should dynamically block access or quarantine user IDs to protect against internal and external threats and also help streamline and automate compliance workflows. The product should be built on a scalable architecture that provides full visibility on data activity across all major databases. Data protection solution shall facilitate:

a) Monitoring and audit of all data activity

b) Real-time security policy enforcement

c) Compliance workflows and audit activities acceleration

d) Support for heterogeneous environments

e) Easy adaptation to changes in data environment

5.1.3. Vulnerability Assessment

Vulnerability Assessment solution shall enable the facility of scanning data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggest remedial actions. The solution shall identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports shall be provided along with suggestions to address all vulnerabilities. It shall detect behavioral vulnerabilities such as account sharing, excessive administrative logins and unusual after-hours' activity. The solution should also have capabilities to identify threats and security gaps in databases that could be exploited by hackers. This solution shall facilitate:

a) Automated discovery of unknown data assets

b) Sensitive data classification in data sources

c) Entitlements and data source credentials monitoring

d) Automated vulnerability scanning and configuration

e) Mapping of predefined tests for best practice standards

f) Behavioral vulnerabilities exposure

g) Vulnerability reporting and action taking

5.1.4. Privileged Access Management

Especially in hybrid cloud environments, a fully managed Privileged Access Management solution must be provided guidance from strategy through steady-state management, and enable automation, analytics and optimization to secure the privileged users.

5.2. User Acceptance Testing (UAT) & Go-Live

After successful implementation of the security system, User Acceptance Testing (UAT) shall be conducted. The SI will be responsible for conducting Encryption Live test for the Data. The User Department may suggest changes/inclusions of minor features before UAT which SI has to do without any financial implications.

The System will be deemed "Live" after successful Encryption Live Test of at least 3 Data Sets of the PDS application

5.3. Training

The SI shall provide hands on training to the personnel as nominated by STPI during the entire process of implementation, go-live and technical support.

5.4. Technical Support Services

The Implementing bidder shall provide Technical Support for the project for a period of 33 months post Go-Live. The SI shall engage Crypto Analyst for providing the Technical Support Services. The activities during this period shall be:

a) Resolution of incidents reported

b) Reporting of Root Cause Analysis

c) Performing advanced activities like:

- Driving Database Activity Monitoring (DAM) product fixes and enhancements
- New system integrations (if any)
- Analyzing and addressing issues related to performance, stability, scalability and extensibility of the systems
- Recommending DAM process improvements as and when required

d) Support Disaster Recovery (DR) Drills.

SI shall not change the deputed manpower without written intimation and approval from STPI. SI shall provide a substitute well in advance if there is any probability of the person leaving the job due to his/her own personal reasons.

The proposed resource should possess the following qualification and skills:

a) **Experience**: 5+ years in Database Activity Monitoring

b) **Skills**:

- Expert knowledge and experience in deploying Database Activity Monitoring using multiple products
- Strong experience in Database Activity Monitoring, Vulnerability Assessment and Encryption
- Should have good integration knowledge
- Basic hand on experience for various databases
- Should be capable of translating Customer business requirement to Technical/ Functional requirement

5.5. Functional Requirement Specification

5.5.1. General Requirements

SL. NO.	Functional Requirements
FR1	The proposed solution should provide easy & fast deployment. It should be available as a pre-deployed virtual appliance which could be deployed on hypervisor like VMware
FR2	The proposed solution Licensing should be based on Active Database Server count
FR3	The proposed solution should not have extra licensing cost for UAT/ Development instances.
FR4	The proposed solution should have a product roadmap.
FR5	The proposed solution should integrate with all type of known databases in the organization

5.5.2. File and Database encryption

SL. NO.	Functional Requirements
FR1	The change of the infrastructure environment should be minimized
FR2	The solution must be capable of being installed without application modification – No DB schema changes (view, index) – No business application changes
FR3	The solution should support various kinds of OS: Unix, Linux, Windows
FR4	The solution should support various kinds of data types – Unstructured data encryption such as WAS log file, backup file, configuration file, image, recording file – DBMS data store encryption

SL. NO.	Functional Requirements
FR5	The solution should support various kind of data format – Large amounts of data – No impact on DB column type and data format (CHAR, INT) – No impact on DB data format and constraint (PK, FK, NULL) – No increase of data size after encryption
FR6	The solution should have the scalability of enterprise environment – Big data environment – Cloud environment
FR7	The solution should possess compatibility of current enterprise environment – Transparent data access via application – Compatibility with backup and replication solutions
FR8	Performance degradation should be minimized
FR9	The solution should have certification and certified encryption algorithms
FR10	The solution should support key management – Full lifecycle of cryptographic keys management such as key generation, access, renewal, destruction should be provided by dedicated key management server and security should be ensured. – The encryption key must be securely protected on a separate server limiting access to the keys
FR11	The solution should support audit and access control – Access control on unauthorized user access to data – Audit log and report

5.5.3. Data Protection for database

SL. NO.	Functional Requirements
FR1	The solution should support integration with the critical databases such as DB2, Oracle, MS-SQL etc.
FR2	The solution should support integration with the Big Data platforms such as Horton Works, Data warehouse such as Exadata etc.
FR3	The solution should offer automatic discovery of databases.
FR4	The solution should provide sensitive data discovery options together with predefined data classification rules for various sensitive data types including PCI data, PII data and offers the ability for customization
FR5	The solution should support user entitlement reviews on database accounts
FR6	The solution should implement blocking – For blocking the solution should be using an agent. – Solution should not be deployed in-line mode for blocking.
FR7	The solution should use agent-based architecture. – The solution agent should perform monitoring, blocking, redaction without any changes on the Database, network configuration & access mechanism.
FR8	The solution should not require any logging to be enabled at the Database level. It should capture full SQL activities without enabling any database level logging.
FR9	The solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes
FR10	The solution should have the ability to monitor data that is passed through encrypted transmissions such as oracle ASO
FR11	The solution should include specialized threat detection analytics that scan and analyze audited data to detect symptoms that may indicate malicious

SL. NO.	Functional Requirements
	stored procedure
FR12	The solution should help in identifying abnormal server and user behavior and providing early detection of possible attacks using outliers. – For example, User activity that is identified as a suspected outlier includes: – User accessing a table for the first time – User selecting specific data in a table that he has never selected before – Exceptional volume of errors. – Activity that itself is not unusual, but its volume is unusual – Activity that itself is not unusual, but the time of activity is unusual. For example, a DBA is accessing a table more frequently than in the past. This could indicate that the DBA
FR13	The solution should support setting up of compliance monitoring. It should have out of box accelerators for PCI/DSS, Data Privacy.
FR14	The solution should have multiple pre-configured policies & reports. Reports should address regulatory compliance such as SOX, PCI DSS, Data Privacy Law, GDPR etc.
FR15	The solution should have easy drag & drop option to customize report without developing or require lot of customization/changes from scratch.
FR16	Reports should be exportable via both PDF and Excel
FR17	All reports generated via the solution should be stored in a secure manner and all alterations to the report generation and to the reports themselves should be auditable
FR18	The solution should provide optimum utilization of resources by using Load balancing between servers. The solution should support Enterprise load balancing
FR19	The solution should support dynamic redaction for privileged user thus certain

SL. NO.	Functional Requirements
	fields such as Aadhaar number, credit card number could be easily hidden from the privileged DBA's.
FR20	The solution should use internal DB to store the Logs.
FR21	The solution should support normalization on the collected audit data thus if a same event occurs in short duration it should increase the count of event rather than creating a new event/log.
FR22	The solution should provide incident management module which will help business- user with workflow automation for tracking and resolving the database security incidents.
FR23	The solution should provide option of filtering option that only specific violation should be sent to SIEM.
FR24	The solution should have Vulnerability Assessment module which can discover unpatched vulnerabilities, default credentials, database default configurations/ misconfiguration.
FR25	The solution Vulnerability reports could be imported on a SIEM solution for providing a centralized vulnerability platform.
FR26	The solution should support integration with SIEM solution.
FR27	Solution must be able to prevent unauthorized activity based on command, table, database, IP, Application/OS/Database user name, time-based etc.
FR28	Proposed solution must be deployed without any network architecture change and down-time.
FR29	Agent should not perform any processing such as normalization of activities. Solution should utilize less than 5% of operating system CPU utilization.
FR30	Solution must have temper-proof log storage capability
FR31	Solution should have flexible policy definition on the basis of who are the users, what they are accessing database/table, time of the day, from where they are

SL. NO.	Functional Requirements
	accessing & how the user is accessing.
FR32	Policy action implementation should be defined.
FR33	Solution should capture SQL errors as well.
FR34	Solution must be capable to scale across multiple location with centralized management
FR35	Solution should be capable to discover database on the network, find and classify sensitive objects in databases.
FR36	Solution should be capable to detect default configurations, vulnerabilities on database without any changes/additional hardware in proposed solution.
FR37	Solution must support filtering/hiding of the bind variables of all the SQL activities captured.
FR38	The solution must identify down to the user level who is accessing which table & what SQL activity is performed by the database user
FR39	The solution should provide means to profile data activity behaviour together with tools to filter noise or known false positives
FR40	Solution must be capable to monitor all type of user activity. This users can be local host, remote, database administrator, application user etc. and allow to configure to prevent specific command/user/table access
FR41	Solution support individual user access auditing for packaged applications, like SAP, PeopleSoft, Siebel
FR42	Audit records should contain all information required for understanding of the event including: Source and destination IP, DB and OS user name, source application, number of affected rows, and database instance name
FR43	The solution should not store sensitive data in logs generated by the application (e.g. passwords)
FR44	Logs and audit-trail generated by the solution should not be editable by users

SL. NO.	Functional Requirements
	and should be read-only
FR45	The solution should provide an internal workflow capability that allows users to raise issues and assign them to other users
FR46	Alerting should be available via email, SNMP and Syslog
FR47	Solution should be capable to integrate with third-party ticketing systems
FR48	Solution should proactively alert the administrators for any type of activity necessary including Syslog, SNMP, emails, and pagers, or custom classes for distribution of alerts
FR49	Solution must support role based access and integration with enterprise directories and RADIUS
FR50	Solution must be able to provide reports about database activity information including who logged in, DB user, application user, OS user, from where, how, etc.
FR51	Solution must be able to monitor and log database traffic that is encrypted with SSL or IPsec.
FR52	Solution must be able to capture complete DML, DDL statements and allow preventing unauthorized connection irrespective type of connection medium and user.
FR53	The solution should detect excessive, unnecessary, unauthorized, suspicious or high risk activity in real-time for both internal and external users including privileged users.
FR54	The solution should provide granular policy management by separate audit and security policies be created and managed at different granularity levels
FR55	Solution should support to create whitelist or exceptions list to ignore monitoring certain items (e.g., ignore a column that has zip codes only). Solution set granular policies down to such levels as table, column, specific application, specific type of database, specific user ID, specific IP address, etc.

SL. NO.	Functional Requirements
FR56	The solution should be able to block excessive, unnecessary, unauthorized, suspicious or high risk activity in real-time for privileged users
FR57	The solution should audit accesses with elevated privileges, such as an administrator or system administrator account
FR58	Solution must support prevention time based policy. Such as time of day/week.
FR59	Solution must be able to perform content scanning for regular expression and patterns.
FR60	Solution must be scalable in distributed environment with centralized console.
FR61	Solution should support integration with LDAP
FR62	Solution must have web based interface.
FR63	Solution must provide a Command-Line-Interface (CLI) for scripting/automation purposes
FR64	The solution should support integration with LDAP (AD)
FR65	The solution should provide database change management workflow enforcing separation of duties and traceability of changes

5.5.4. Privileged Access Management

#	Functional Requirement
Platform Delivery	
PD 1.1	The proposed solution must be deployable on-premise, hybrid, and provided as a cloud offering.
PD 1.2	On-Prem: The proposed solution must support a manual installation method on the organizations standard O/S images.
PD 1.3	On-Prem: The proposed solution must support an automated installer on the organizations standard O/S images.

#	Functional Requirement
PD 1.4	Hybrid: The proposed solution architecture support spanning multiple datacenters across on-prem and private cloud resources.
PD 1.5	Cloud: The proposed solution must be delivered by the principal as a Software as a Service (SaaS) cloud delivery model. Please describe your cloud delivery model.
PD 1.6	The proposed solution must be hypervisor agnostic and not rely on physical or virtual appliances.
Platform Architecture	
PA 1.1	The proposed solution must be built around industry standard Linux or Microsoft technology.
PA 1.2	The proposed solution cannot rely on non-standard or proprietary components such as non-commercially available databases or network protocols.
PA 1.3	Describe the proposed solutions full architecture stack for on-prem and cloud delivery models.
PA 1.4	The proposed solution must include components to distribute workloads across an environment.
PA 1.5	Describe the proposed solutions scale-out architecture properties.
PA 1.6	The proposed solution must not rely on Windows Server Failover Clusters for High-Availability of the presentation layer (front-end web portal).
PA 1.7	Describe the proposed solutions high-availability architecture for on-prem and cloud delivery models.
PA 1.8	Describe the proposed solutions disaster recovery features for on-prem and cloud delivery models.
PA 1.9	The proposed solution must support a wizard driven upgrade process and be performed without vendors professional services.
PA 1.10	The proposed solution must run on the latest and fully patched version of Microsoft's Operating System at all times.
Credential Management	

#	Functional Requirement
CM 1.1	The proposed solution must support the following types of accounts for password changing out-of-the-box:
CM 1.2	Active Directory (All Account)
CM 1.3	Windows Local User & Administrative Accounts (2008 R2+)
CM 1.4	Linux Local User & Administrative Accounts (Any Distribution)
CM 1.5	Unix Local Users & Administrative Accounts (Any Distribution)
CM 1.6	Network System Accounts - Please list your supported devices
CM 1.7	Hypervisors (Hyper-V & VMware)
CM 1.8	Out-of-Band Management Systems (iDrac & HP iLO)
CM 1.9	AWS IAM Access Keys
CM 1.10	MS Azure Office 365 / AD Accounts
CM 1.11	Google Cloud Platform
CM 1.12	SSH Keys - Please list how SSH Keys are managed in the proposed solution
CM 1.13	Database Accounts - Please list your supported databases
CM 1.14	LDAP Accounts - Please list your supported directory stores
CM 1.15	Mainframe Accounts - Please list your supported mainframe systems
CM 1.16	Network Information Service Directory Account
CM 1.17	The proposed solution must allow for the application owner to add additional credential management functions, e.g., connecting to legacy equipment through telnet to update account information, or updating credentials in a file on a remote host. Please describe how your solution meets addresses this requirement.
Access Control	
AC 1.1	The proposed solution must have a native integration with Active Directory

#	Functional Requirement
	and support LDAP(s).
AC 1.2	The proposed solution must integrate with Active Directory Security Groups as a component of the role-based access control.
AC 1.3	The proposed solution's Active Directory Integration must be capable of automating new user onboarding.
AC 1.4	The proposed solution must allow for Integrated Windows Authentication for platform authentication.
AC 1.5	The proposed solution must support Local authentication & Local role-based access control groups.
AC 1.6	The proposed solution must support any SAML 2.0 Identity Provider for Single Sign-on.
AC 1.7	The proposed solution must support any RADIUS-based multi-factor authentication solution.
AC 1.8	The proposed solution must support out-of-the-box integrations with DUO, FIDO2, and any TOTP solution. Please list supported MFA solutions.
AC 1.9	The proposed solution must support IP Address whitelisting for access users.
AC 1.10	The proposed solution must support masking available login domains during the login process from the user.
AC 1.11	The proposed solution must support a custom informational banner at the login screen without having to modify CSS files.
AC 1.12	The proposed solution must be configurable to force connections to the platform to use HTTPS only.
Policy Management & Workflows	
PMW 1.1	The proposed solution must support a single pane of glass for policy configuration across an entire deployment.
PMW 1.2	The proposed solution's policy configuration must include the ability to configure items such as credential management settings, security settings,

#	Functional Requirement
	and locations/vaults for workload assignment.
PMW 1.3	The proposed solutions must support applying policies at a group or individual account level.
PMW 1.4	The proposed solution must support the below listed workflows. Please describe any additional workflow capabilities not listed.
PMW 1.5	Justification for Access (user must submit a reason/comment before accessing)
PMW 1.6	Access Approval (single and/or multi-tiered).
PMW 1.7	Account Check Out (one-time password)
PMW 1.8	Just-in-Time Administration
PMW 1.9	Dual Control (four-eyes principle)
PMW 1.10	Please describe the proposed solutions ability to support modifications to any existing workflows through scripting if applicable.
PMW 1.11	The proposed solution's Check Out function must support manual, forced, and an automatic time-based check in process.
PMW 1.12	The proposed solutions justification and approval workflows must support optionally validating case/tickets with an external ticketing system during the justification and approval process.
PMW 1.13	Does the solution offering the ability to extend upon features for out-of-the-box case/ticket validation integrations, e.g., validating requesters IP address? If so, how is this accomplished?
Auditing & Reporting	
AR 1.1	The proposed solution must include a tamper-proof, robust, audit of all activities within and against the platform.

#	Functional Requirement
AR 1.2	The proposed solution's audit must provide the who, what, where, and when of activity. Please describe any additional data which is captured to supplement the audit trail.
AR 1.3	The proposed solution must support forwarding logs to a SIEM platform. Please describe any additional integration points if there exists any outside of standard log forwarding.
AR 1.4	The proposed solution must support keystroke capturing for Linux, Unix, and Windows Operating Systems.
AR 1.5	The proposed solution must support the cross-searching of keystrokes and allow exporting for archiving.
AR 1.6	The proposed solution must support reviewing the audit trail under a single pane of glass portal.
AR 1.7	The proposed solution must include pre-configured reports. Please describe how many and the type of reports provided out-of-the-box.
AR 1.8	The proposed solution must offer the application owner the ability to create custom reports without vendor services. Please describe how the solution meets this requirement.
AR 1.9	The proposed solution must include a behavior analytics component or accompanying solution.
AR 1.10	The analytics platform must provide informative dashboards include top users, top accounts, alerts, warnings, etc. Please describe what type of dashboards, reports, or other informative information is available for the platform.
AR 1.11	The analytics platform must provide a watch list for users whose activity may be suspicious.
AR 1.12	The analytics platform must provide an audit trail of Security Admins reviewing and responding to alerts.
AR 1.13	The analytics platform must provide historical data of user activities.

#	Functional Requirement
AR 1.14	The analytics platform must provide a method to visualize users who access similar accounts.
AR 1.15	The analytics platform must provide a method to visualize user access geography/IP.
AR 1.16	The analytics platform must provide behavior analytics to applications making request through the PAM API.
AR 1.17	The analytics platform must provide an automated remediation process against anomalous activity in the PAM solution supporting the below. Please list any additional notification or remediation actions if not listed below.
AR 1.18	Email notification
AR 1.19	Multi-factor Authentication
AR 1.20	Account Lockout
AR 1.21	Recording Session
AR 1.22	Account Demotion (Removing admin rights on account based on threat)
AR 1.23	Ability to integrate with external platforms such as Ticketing Systems and SIEM solutions. Please describe what integration approach is used for the analytics platform.
AR 1.24	The analytics platform & PAM platform must provide all reporting functions within the single pane of glass portal without the need for external reporting platforms such are Crystal Reports or SQL Server Reporting Services.
AR 1.25	Does the analytics platform support customized dashboards?
AR 1.26	Does the analytics platform support external data sources for analysis?
AR 1.27	Please describe the analytics platform delivery model.
PS 1.1	The proposed solution must support monitoring a session without notifying the connected user.
PS 1.2	The proposed solution must support sending a message to an active user

#	Functional Requirement
	session.
PS 1.3	The proposed solution must support terminating an active user session.
PS 1.4	The proposed solution must provide pre-configured methods for session connections such as RDP, SSH, Mainframe Emulators, PowerShell, and SSMS. Please list the out-of-the-box session connectors.
PS 1.5	The proposed solution must allow the application owner the ability to add custom session connectors session launchers to be configured from the single pane of glass interface without the need for vendors professional services.
PS 1.6	The proposed solution must not require middleware applications such as AutoIt, AutoHotkey, or other Windows GUI automation platforms to add custom application session launching.
PS 1.7	The proposed solution must support launching to session connections without disclosure of the account password.
PS 1.8	The proposed solution must support the automatic recording of session connectors with and without notification to the user.
PS 1.9	The proposed solution must support capturing Windows application events for active user sessions.
PS 1.10	The proposed solution must support cross-searching for executed Windows processes, e.g., opening PowerShell, or MMC.
PS 1.11	The proposed solution must provide a method of recording sessions initiated outside the PAM solution. Please describe how this requirement is met.
PS 1.12	The proposed solution must support cross-searching for captured keystrokes.
PS 1.13	The proposed solution must provide a method of whitelisting commands issued to SSH-based resources.
PS 1.14	The proposed solution must support offloading recordings to a SAN, NAS, or other network shares while still being encrypted.
PS 1.15	The proposed solution must support a configuration where RDP & SSH sessions are brokered through the PAM "jumpbox" component. Please

#	Functional Requirement
	describe how this workflow is accomplished and what architectural components are necessary.
PS 1.16	The proposed solution must support a configuration where RDP & SSH sessions do not require a "jumpbox" component to facilitate connections. Please describe how this is accomplished.
PS 1.17	If the proposed solution has a "jumpbox" component, does it support automatic load balancing and automated failovers. Please described how the solution meets this requirement.
Account Discovery	
AD 1.1	The proposed solution must include an automated account discovery function. Please describe how the solution meets this requirement.
AD 1.2	The proposed solution's account discovery function must allow for scheduling. Please describe how granular and flexible account discovery can be scheduled.
AD 1.3	The proposed solution's account discovery function must provide a method to visualize discovery accounts across the environment which include hostname, account name, operating system, and account permission. Please describe any other data capture which can be visualized through the solutions account discovery.
AD 1.4	The proposed solutions account discovery function must provide out-of-the-box support for Active Directory Accounts, Windows Accounts, Linux Accounts, Unix Accounts, Hypervisor Accounts. Please list any other systems, devices, or platforms out-of-the-box account discovery supports.
AD 1.5	The proposed solution's account discovery function must support flexible automated onboarding of discovered accounts. Please describing the solutions automate onboarding feature for discovered accounts.
AD 1.6	The proposed solution's account discovery function must allow for application owners to add custom discovery objects for systems, platforms, and devices not supported out-of-the-box. Please describe how the platform can meet this requirement.
API & Integration	

#	Functional Requirement
AI 1.1	The proposed solution must offer an extensive web services API with create, read, update, and delete functions. Please decribe the solutions API offering.
AI 1.2	The proposed solution's web services API must support Integrated Windows Authentication and OAuth Authentication.
AI 1.3	The proposed solution's web services API must support IP address whitelisting.
AI 1.4	The proposed solution's web services API use must be auditable by the PAM platform.
AI 1.5	The proposed solution must offer a SDK or programming libraries for inclusion within the source code of internally developed software. Please describe how the solution meets this requirement.
AI 1.6	The proposed solution's SDK/programming libraries must support IP address whitelisting.
AI 1.7	The proposed solution's SDK/programming libraries must be auditable by the PAM platform. Please describe what data is captured in the audit for this function.
AI 1.8	The proposed solution's SDK/programming libraries must offer a configurable encrypted cache to limit calls to the PAM solution.
AI 1.9	The proposed solution's SDK/programming libraries audit must be accessible within the PAM platform.
AI 1.10	Java is restricted within the domain; the proposed solution's SDK/programming libraries or other API components must offer a non-Java solution to meet this requirement. Please describe the solutions ability to meet this requirement.
AI 1.11	Does the proposed solution offer a client or method for accessing the PAM platform through a command-line interface? If so, please describe how this method can be secured against abuse.
AI 1.12	Please describe the proposed solutions method for securing SDK/programming libraries communication, authentication, and means of

#	Functional Requirement
	protecting against abuse.
AI 1.13	The proposed solution must provide a SCIM interface/connector for integration into IdAM platforms. Please describe how SCIM is applied in the solution.
AI 1.14	The proposed solution must have an integration with common vulnerability management solutions for offloading credentials required in authenticated scans. Please list supported out-of-the-box vulnerability management solutions.
AI 1.15	The proposed solution must support integration with common ticketing and case management systems. Please list supported out-of-the-box ticketing and cases management solutions.
AI 1.16	Please list the proposed solutions integration points or integration methodology.
Security	
SC 1.1	The proposed solution must protect data at rest. Please describe how the proposed solution meets this requirement.
SC 1.2	The proposed solution must protect data in motion. Please describe how the proposed solution meets this requirement.
SC 1.3	The proposed solution must provide a user report; allowing admins to visualize what accounts an offboarded individual touched. Please describe how the solution meets this requirement.
SC 1.4	The proposed solution must provide an easy method to update passwords for the accounts touched in the user report mentioned previously.
SC 1.5	Transparent Data Encryption is used on all organizational databases; the proposed solution's backend database must support Transparent Data Encryption.
SC 1.6	The proposed solution must support offloading the management of the master encryption key to Hardware Security Module. Please list supported out-of-the-box Hardware Security Module solutions.

#	Functional Requirement
SC 1.7	The proposed solution must offer a built-in scheduled backup function capable of saving to a SAN, NAS, or other network location. Please describe how the proposed solution meets this requirement.
SC 1.8	The proposed solution must support configurable disclosure messages for errors to prevent data leakage. Please describe how the proposed solution meets this requirement.
SC 1.9	The organization uses non-standard ports for a variety of platforms; the proposed solution must support configurations to allow for non-standard ports. Please describe how the solution meets this requirement and what components are configurable.
SC 1.10	The proposed solution must support a customizable password complexity and rules engine.
SC 1.11	The proposed solution must support allowing our standard organizational Group Policy Objects to be enforced on all components of the platform architecture.
User Experience	
UX 1.1	The solution must provide a single-pane of glass interface for all access and configurations for all functions, e.g., administration, auditing, reporting, vaulting, policies, session connectors, account discovery, and web services.
UX 1.2	The solution must not require browsers plugins (Flash, Java, etc.) for any function of accessing, initiating, reviewing, administration, or management.
UX 1.3	The proposed solution's user experience should be the same for all users, administrators, and auditors to streamline training and adoption. Please explain the user experience across components of the solution for auditing, vaulting, session connectors, administration, behavior analytics, and any other component of the solution not listed.
UX 1.4	Please describe the solutions ability to provide accessibility to users to meet 503c compliance.
UX 1.5	The proposed solution's account segregation system should be simple and intuitive for all users of the platform to streamline training and adoption.

#	Functional Requirement
	Please describe how the solution meets this requirement.
UX 1.6	The proposed solution's account segregation system should support an inheritance model. Please describe how the solution meets this requirement.
Session Management	
SM 1.1	The solution should be able to manage and interact with multiple remote sessions for both Remote Desktop Protocol (RDP) and SSH in an unified environment.
SM 1.2	The solution should be able to manage multiple sessions active at once, using different connection protocols and a variety of privileged accounts.
SM 1.3	The solution should be able to launch and configure sessions across multiple environments with credentials automatically injected into sessions as needed.
SM 1.4	The solution should be able to provide an end to end record of privileged user access and provide a collaboration between teams to view live and send messages
SM 1.5	The solution should provide custom terminal banners after a successful login with available commands to be displayed.
SM 1.6	The solution should have the ability to start a terminal connection and launch using a single line and include 2FA for access.
SM 1.7	The solution should be able to utilize built in capabilities such as the up and down arrows for command history.
SM 1.8	The solution should not require more hardware or additional licensing for these terminal connection features.
DevOps Security	
DSV 1.1	A DevOps platform should provide a scale out platform for high transactional API calls. What type of scalability and performance does the solution provide?
DSV 1.2	When utilizing a solution for developers; what are the recommended components for a successful deployment?
DSV 1.3	Developers require different methods to store credentials; what are the credential storage options available with the solution?

#	Functional Requirement
DSV 1.4	Developers require different methods for authenticating into their vault; what types of authentications methods are available in the DevOps Security solution?
DSV 1.5	What Vault integrations are currently supported?
DSV 1.6	The solution requires SOC II.
DSV 1.7	For a high latency connection many vendors provide other methods to provide credentials to their applications; what methods are available in the solution to work through these types of issues?
DSV 1.8	What is the business continuity plan for DevOps Security platform?

6. Bill of Quantity

Below table describes the bill of material, which will be used for this project:

Sl. No.	Item	Unit	Qty
1	Data Protection for Databases	License	3
2	Vulnerability Assessment for Databases	License	3
3	Node Level Software License for Data Protection	License	2
4	Server Level Software License for Data Protection	License	1
5	File and Database Encryption	License	3
6	Data Encryption Key Management	License	3
7	Privilege vault on-premises for privileged users	License	45
8	Server Hardware in High Availability (For Server level License)	No	4

Sl. No.	Item	Unit	Qty
9	Server Hardware in High Availability (For Node level License)	No	3

7. Roles & Responsibility

Sl. No.	Activity	SI	STPI/ FSC&W
1.	Procurement & Implementation of Security Solution	✓	
2.	Engagement of Technical resources for installation, configuration and support	✓	
3.	Meet performance obligations as per SLA and RFT	✓	
4.	Release payment as per payment terms		✓
5.	Necessary Permissions & Clearances		✓
6.	Provide all necessary IT Infrastructure for installation of the solution		✓
7.	Coordination for SDC and Near DR Access		✓

8. Project Schedule

Sl. No.	Activity/ Milestone	Timeline
1.	System Study/ Requirement Gathering	T_0 + 15 days
2.	Submission of Inception Report	T_0 + 20 days
3.	Procurement & Delivery of COTS Solution (Security Licenses)	T_0 + 45 days
4.	Procurement & Delivery of Servers for Security	T_0 + 75 days
5.	Installation, Commissioning & Implementation of Data Encryption Solution for Department of Food	T_0 + 90days

Sl. No.	Activity/ Milestone	Timeline
	supplies and Consumer Welfare	
6.	UAT & Go-Live	$T_1 = T_0 + 105$days
7.	Technical Support Services	T_1 + 33months

T_0= Date of Award of Contract

9. Payment Terms

Payment to the SI shall be made as per below schedule -

Sl. No.	Payment Schedule	% Payment
1.	Procurement & Delivery of COTS Solution (Security Licenses)	90% of basic cost proposed for Procurement of Security Licenses and 100% tax amount
2.	Procurement & Delivery of Servers for Security	80% of basic cost proposed for Procurement of Servers for Security and 100% tax amount
3.	Installation, Commissioning & Implementation	80% of basic cost proposed for Implementation of Security in FS&CW System and 100% tax amount
4.	UAT & Go-Live	Balance 10% of Sl.No. 1 Balance 20% of Sl.No. 2 & 3
5.	Software Assurance (SA) of Security Licenses	100% payment annually in advance
6.	Technical Support (Crypto-Analyst)	To be paid on monthly basis on completion

Terms:

a) Payment shall be made against submission of invoices accompanied by proof of delivery and installation report certified by the client/ client nominated authority.

b) Invoice shall be generated in the **n**ame of **"Department of Food supplies and Consumer Welfare, Govt. of Odisha"** through **"Director, Software Technology Park of India, Bhubaneswar"**

c) All costs quoted by the SI shall be inclusive of taxes / levies. However, the taxes shall be applicable at the prevailing rate at the time of billing.

d) Any change is taxes shall be paid additionally over and above the agreed cost.

10. Forms & Annexure

10.1. Technical Bid Cover Letter

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Subject: Proposal for the RFT for Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha

Reference No.: <<RFT No. >>

Dear Sir/Madam,

We, the undersigned, offer to provide Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha project.

We are hereby submitting our Proposal, which includes the Technical Proposal and the Commercial Proposal sealed in separate envelopes.

We hereby declare that all the information and statements made in this Technical Proposal are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Proposal is accepted, to initiate the Implementation services related to the assignment not later than the date indicated in the RFT Document.

We agree to abide by all the terms and conditions of the RFT document. We would hold the terms of our bid valid for 180 days from the date of submission of bid as stipulated in the RFT document.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: _____

Name and Title of Signatory: _____

Name of Firm: _____

Address: _____

10.2. Self-Declaration: Not Blacklisted (in company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

In response to the RFT No. <<RFT No.>>, for RFT titled "Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project", I/ We hereby declare that presently our Company/ firm is not under declaration of ineligibility for corrupt & fraudulent practices, blacklisted either indefinitely or for a particular period of time, or had work withdrawn, by any State/ Central government/ PSU.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender, if any to the extent accepted, may be cancelled.

Thanking you,

Name of the Bidder: .....

Authorized Signatory: .....

Signature:

Seal:

Date:

Place:

10.3. Bidder's Authorization Certificate

(Company letter head)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Subject: Proposal for the RFT for Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project

Reference No.: <<RFT No.>>

Sir,

<Name>, , <Designation> is hereby authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing the above said Bid. S/He is also authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing above said application For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Name of the Bidder: -

Verified Signature:

Authorized Signatory: -

Seal of the Organization: -

Date:

Place:

10.4. Acceptance of Terms& Conditions/Clauses

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Sir,

I have carefully and thoroughly gone through the Terms & Conditions contained in the RFT Document [<<RFT No.>>] regarding Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project.

I declare that all the provisions/clauses of this RFT/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Thanking you,

Name of the Bidder: .....

Authorized Signatory: .....

Signature:

Seal:

Date:

Place:

10.5. Format for fairness of documents

(Company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Sir

In response to the RFT No. <<RFT No.>> titled "Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project", I/ We hereby declare that any documents or information submitted under this bid is without any doubt, true and fair, to the best of my/our knowledge.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Thanking you,

Name of the Bidder: -

Authorized Signatory: -

Seal of the Organization: -

Date:

Place:

10.6. Financial Bid Format

10.6.1. Financial Proposal Submission Form

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Subject: Proposal for the RFT for Selection of Bidder for Installation, Commissioning and Maintenance of Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project

Reference No.: <<RFT No. >>

Dear Sir/Madam,

We, the undersigned, offer to provide Installation, Commissioning and Maintenance services for Data Encryption Solution for Department of Food Supplies and Consumer Welfare, Govt. of Odisha Project.

Our attached Financial Proposal is for the sum of <<Amount in words and figures>>inclusive of taxes and duties.

1. PRICE AND VALIDITY

All the prices mentioned in our Tender are in accordance with the terms as specified in the RFT documents. All the prices and other terms and conditions of this Bid are valid for a period of 5 years from the date of opening of the Bid.

We understand that the actual payment would be made as per the existing tax rates during the time of invoicing.

2. TENDER PRICING

We further confirm that the prices stated in our bid are in accordance with your clauses in RFT/Tender document.

3. QUALIFYING DATA

We confirm having submitted the information as required by you in your RFT. In case you require any other further information/ documentary proof in this regard

before/during evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

4. BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified.

5. PERFORMANCE BANK GUARANTEE

We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee as specified in the RFT document.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.

We understand you are not bound to accept any Proposal you receive.

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive.

Thanking you,

We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

10.6.2. Summary Cost

SL. NO.	Components	Total (Including GST @18%)
A	Procurement & Implementation of Security Solution in Department of Food supplies and Consumer Welfare (Year-1)	
B	Operational Expense along with Software Assurance (Year-2)	
C	Operational Expense along with Software Assurance (Year-3)	
	Total (in Figures)	
Total (in Words)		

10.6.2.1. Procurement &Implementation of Security Solution in Department of Food supplies and Consumer Welfare (Year 1)

SL. NO.	Capital Expenses (Year-1)	Unit	Qty	Basic Cost	GST @ 18%	Total
1.	Procurement of Security Licenses					
1.1.	Procurement & Delivery of Security Licenses	Lot	1			
1.2.	Set-up and configuration of Security Licenses	Location	2			
2.	Procurement of Servers for Security					
2.1.	Procurement & Delivery of Servers for Security	Lot	1			
2.2.	Set-up and configuration of Servers for Security	Location	2			
3.	Implementation of Security in the application	Location	2			
4.	Technical Support (Crypto Analyst)	Man-Month	9			
Total (in Figures)						

SL. NO.	Capital Expenses (Year-1)	Unit	Qty	Basic Cost	GST @ 18%	Total
Total (in Words)						

10.6.2.2. Operational Expenses (Year 2)

SL. NO.	Recurring Expenses (Year-2)	Unit	Qty	Basic Cost	GST @ 18%	Total
a	Software Assurance (SA) of Security Licenses	Lot	1			
b	Technical Support	Man-Month	12			
Total (in Figures)						
Total (in Words)						

10.6.2.3. Operational Expenses (Year 3)

SL. NO.	Recurring Expenses (Year-2)	Unit	Qty	Basic Cost	GST @ 18%	Total
a	Software Assurance (SA) of Security Licenses	Lot	1			
b	Technical Support	Man-Month	12			
Total (in Figures)						
Total (in Words)						

11. Annexure I: Current Scenario

11.1. Stakeholders

Secure and robust IT infrastructure has been installed at SDC, for streamlining the administrative processes to improve the service delivery standards in FS&CW. The key stakeholders for the projects are:-

- Food Supplies & Consumer Welfare Department
- District Civil Supplies Officers
- Odisha State Civil Corporations Limited
- State Project Management Unit
- Other Government Officials

11.2. IT Infrastructure at OSDC

11.2.1. Server Infrastructure

A dedicated server environment is installed at OSDC in a co-location mode. The Server infrastructure is provided by Department and other infrastructure like Network, Storage, Power, Security and cooling are provided by OSDC. The necessary security policy is followed for this organization. The server infrastructure is given below:

Application/Web Server: The application servers are configured with Load-balancing mode. The hardware load balancer of OSDC is used for this purpose. Multiple applications are running in the servers. The load balancer is configured to distribute the load between multiple application servers. Necessary configuration on forwarding request is done in the load balancer.

The environment used by the proposed applications are given below.

#	Application	SI	Front-End	Back-End
1	Ration Card Management System (RCMS)	CSM	.NET	MS SQL
2	FPS Automation System	Link Well	.NET	MS SQL
3	Supply Chain Management System	CSM	Java	MS SQL
4	SAP	SAP	SAP	SAP
5	Grievance Redressal Management System	CSM	.NET	MS SQL

#	Application	SI	Front-End	Back-End
6	Food Odisha Portal	CSM	.NET	MS SQL
7	Paddy Procurement Automation System	CSM	Java	MS SQL
8	MDM	IBM	-	MS SQL
9	PIMS	TQM	Java	MS SQL
10	DLM	CSM	.NET	MS SQL

Database Server: The database servers are configured in cluster mode. Two servers are configured dedicatedly for this purpose. Another DB server is configured in standalone mode for backup purpose.

Document Server: As the applications are configured in load-balancing mode, a common document server is maintained for all application servers. The document server is configured in sharing mode.

Staging server: The staging server environment is available for application, web and DB servers. All the testing and modifications are done in this server before going to live server environment.

Server Hardware

Servers			CPU	RAM	HDD	Purpose	Status
A	Blade Server-I	HP BLc7000					
1	HP BL460C G9 Blade	HP BLADE SERVER 1	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
2	HP BL460C G9 Blade	HP BLADE SERVER 2	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
3	HP BL460C G9 Blade	HP BLADE SERVER 3	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
4	HP BL460C G9 Blade	HP BLADE SERVER 4	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
5	HP BL460C G9 Blade	HP BLADE SERVER 5	8Core x 2	128GB	600GB x 2 Raid1	VM	Active

Servers			CPU	RAM	HDD	Purpose	Status
6	HP BL460C G9 Blade	HP BLADE SERVER 6	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
7	HP BL460C G9 Blade	HP BLADE SERVER 7	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
8	HP BL460C G9 Blade	HP BLADE SERVER 8	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
9	HP BL460C G9 Blade	HP BLADE SERVER 9	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
10	HP BL460C G9 Blade	HP BLADE SERVER 10	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
11	HP BL460C G9 Blade	HP BLADE SERVER 11	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
12	HP BL460C G9 Blade	HP BLADE SERVER 12	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
13	HP BL460C G9 Blade	HP BLADE SERVER 13	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
14	HP BL460C G9 Blade	HP BLADE SERVER 14	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
15	HP BL460C G9 Blade	HP BLADE SERVER 15	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
16	HP BL460C G9 Blade	HP BLADE SERVER 16	8Core x 2	128GB	600GB x 2 Raid1	VM	Active
B	Rack Server						
17	HP DL560 Gen8 Rack	HP Rack SERVER 1	8Core x 4	256GB	1.7TB Raid5	Database	Active
18	HP DL560 Gen8 Rack	HP Rack SERVER 2	8Core x 4	256GB	1.7TB Raid5	Database	Passive
19	HP DL380 Gen9 Rack	HP Rack SERVER 2	8Core x 2	128GB	1.7TB Raid5	Database	Active

Servers			CPU	RAM	HDD	Purpose	Status
C	Blade Server-II	Dell MX7000 CHASIS 2					
1	Dell Power Edge MX740c	Dell BLADE SERVER 1	18Core x 2	575GB	2.4TB Raid5	VM	Active
2	Dell Power Edge MX740c	Dell BLADE SERVER 2	18Core x 2	575GB	2.4TB Raid5	Database	Active
3	Dell Power Edge MX740c	Dell BLADE SERVER 3	18Core x 2	575GB	2.4TB Raid5	Database	Passive
4	Dell Power Edge MX740c	Dell BLADE SERVER 4	16Core x 2	375GB	2.4TB Raid5	VM	Active
5	Dell Power Edge MX740c	Dell BLADE SERVER 5	16Core x 2	375GB	2.4TB Raid5	VM	Active
6	Dell Power Edge MX740c	Dell BLADE SERVER 6	16Core x 2	375GB	2.4TB Raid5	VM	Active
7	Dell Power Edge MX740c	Dell BLADE SERVER 7	16Core x 2	375GB	2.4TB Raid5	VM	Active
8	Dell Power Edge MX740c	Dell BLADE SERVER 8	16Core x 2	375GB	2.4TB Raid5	VM	Active

11.2.2. Other Infrastructure

Storage Environment: The database and document servers are connected to the SAN storage available at OSDC. They are facilitated with 10 TB storage each.

Backup Environment: As both application and database files are stored centrally at the SAN, provided by OSDC, so the backup policy of OSDC is followed for this application. The incremental and full back up is taken periodically as per policy.

Network Environment: As the servers are configured inside OSDC, so the network of OSDC is used for accessing the servers. The necessary configuration of Firewall and Network switch is configured for the servers and storage.

Internet: NKN internet is used in SDC to facilitate the WAN connection to all the applications hosted.

DR Provision: The SDC storage is connected with NDC. The replication of data has been done into NDC. The Near DC is configured at STPI DC. The replication of data is also plan to done at this location.

11.2.3. Software

#	Software	Details	Qty
1	Operating System	Windows server 2012 R2 Standard	16
2	Operating System	Windows server 2012 R2 Data Centre	3
3	RDBMS	MS SQL Server 2012 Enterprise Edition	2

11.2.4. Application/Websites

#	Software	Details
1	Website	www.foododisha.in
2	Application	https://Portal.pdsodisha.gov.in
3	Application	https://Pdsodisha.gov.in
4	Application	https://Ppas.pdsodisha.gov.in
5	Application	https://Dlm.pdsodisha.gov.in
6	Application	https://scms.pdsodisha.gov.in
7	Services	API Services

11.2.5. Modules running in the servers

Currently different applications are being used for managing and monitoring all related operations in the state. The application manages end-to-end solution to business critical problems. Most of them run on web platform on a 24X7 service delivery basis. The various modules constituting the system are:

#	Application	Activities
1	Ration Card Management System (RCMS)	Ration Card Registration/Addition/Deletion Allotment order generation

#	Application	Activities
2	FPS Automation System	Distribution to beneficiaries through POS
3	Supply Chain Management System	Distribution from RRC to FPS
4	SAP	Internal Accounts & Material Management
5	Grievance Redressal Management System	Portal to beneficiaries for raising grievance
6	Food Odisha Portal	Distribution from Miller to RRC & Farmer Registration
7	Paddy Procurement Automation System	Distribution from PACS to Miller
8	MDM Tool	Used internally to find out the De-Duplication
9	PIMS	Internal Payroll and HR Management
10	DLP	Verification of Weights & Measurements by Legal Metrology Officers.

11.2.6. Current Storage Size

DB Size	10 TB
Replication DB	10 TB
Staging DB	-
App	100 GB
Document (pdf)	1 TB
Space Allocated	15 TB

11.3. IT Infrastructure at STPI DC

The Near DC has been planned to execute at STPI DC. The below IT Infra has been planned to deployed for this project. This expected to be completed by December 2019.

11.3.1. Server Infrastructure

#	Server	Qty	Details
1	Application Server	4	Dell Power Edge MX740c, 18Core x 2 Processor
2	Database Server	1	Dell Power Edge MX740c, 18Core x 2 Processor
3	File Server	-	
4	Other Server	-	

11.3.2. Other Infrastructure

a) 10 TB SAN Storage has been provisioned dedicatedly to this environment.

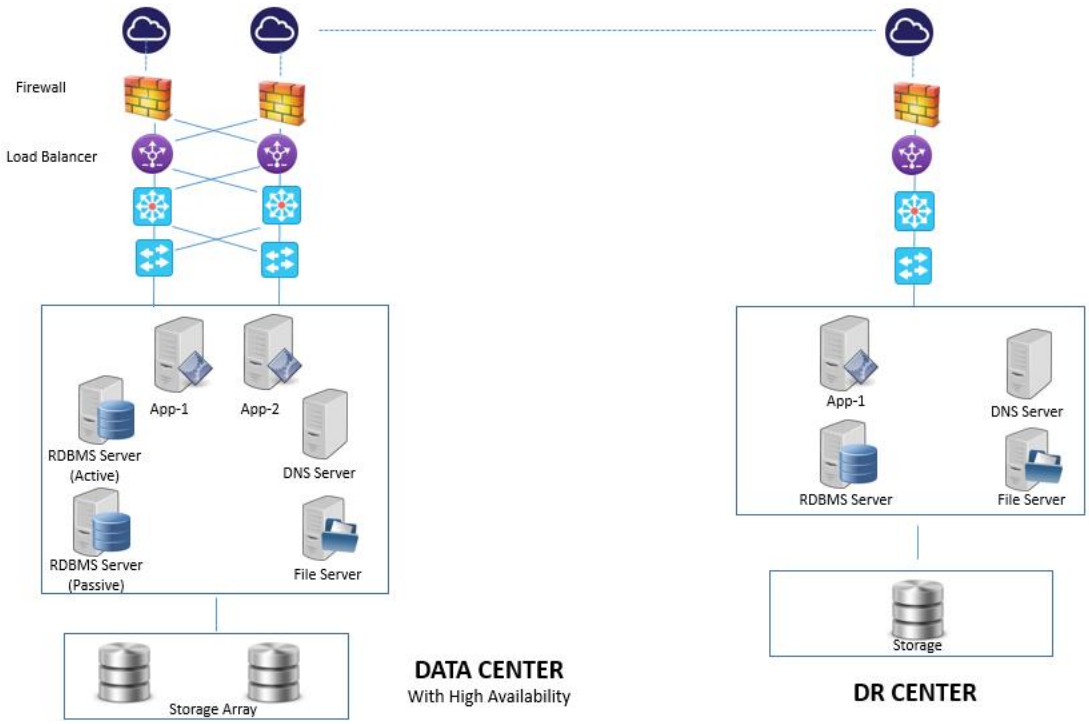
b) STPI has provided the Internet Connectivity to the servers.

c) The MPLS connectivity is configured from STPI DC to OSDC

d) Other Facilities are provided by STPI

11.3.3. Software

#	Software	Details	Qty
1	Operating System	Windows server 2012 R2 Data Centre	4
2	Operating System	Windows server 2012 R2 Standard	1
3	RDBMS	MS SQL Server 2012 Enterprise Edition	1



11.4. Security Requirement

The requirements of data security for this solution are.

a) Classification of sensitive data related to data protection.

b) Real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data.

c) Protects against unauthorized data access by learning regular user access patterns

d) Provide real-time alerts on suspicious activities.

e) Dynamically block access or quarantine user IDs to protect against internal and external threats

f) Support both SQL and non-SQL database

g) Data Protection for Files

h) Help the right users have the right access to the right unstructured data.

i) Data Protection for Files supports file

j) Continuous monitoring and real-time security and protection policies protect unstructured data across the enterprise.

k) Encryption capabilities to help protect file and database data on-premises from misuse.

l) Separation of duties, so that administrators do not have free access to sensitive data.

m) Encrypting file and database data helps organizations meet government and industry compliance regulations.

n) This offering performs encryption and decryption operations with minimal performance impact and high scalability for heterogeneous environments.

o) Event and Log Monitoring