Directorate of Income-Tax (Systems)

Income-Tax Department

Government of India

New Delhi

Request for Proposal (RFP) for Selection of System Integrator for Supply, Installation, Commissioning and Maintenance of CCTV Surveillance, Access Control and Security Scanning System at Aayakar Bhawan, Vaishali, Ghaziabad

Volume- II

Master Service Agreement

Disclaimer

This Request for Proposal (RFP) is issued by the Directorate of Income Tax (Systems).

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither DIT(S), nor any of its officers or employees, nor any of their advisers nor consultants accept any liability or responsibility for the accuracy, reasonableness or completeness of, or for any errors, omissions or misstatements, negligent or otherwise, relating to the RFP or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information contained in this RFP is selective and is subject to updating, expansion, revision and amendment at the sole discretion of DIT(S). It does not, and does not purport to, contain all the information that a recipient may require for the purposes for making a decision for participation in this process. Neither DIT(S) nor any of its officers, employees nor any of its advisors nor consultants undertakes to provide any Party with access to any additional information or to update the information in this RFP or to correct any inaccuracies therein which may become apparent. Each Party must conduct its own analysis of the information contained in this RFP, to correct any inaccuracies therein and is advised to carry out its own investigation into the proposed Project, the regulatory regime which applies thereto and by and all matters pertinent to the Project and to seek its own professional advice on the legal, financial and regulatory consequences of entering into any agreement or arrangement relating to the Project.

This RFP includes certain statements, estimates, projections, targets and forecasts with respect to the Project. Such statements estimates, projections, targets and forecasts reflect various assumptions made by the management, officers and employees of DIT(S), which assumptions (and the base information on which they are made) may or may not prove to be correct. No representation or warranty is given as to the reasonableness of forecasts or the assumptions on which they may be based and nothing in this RFP is, or should be relied on as, a promise, representation or warranty.

ABBREVIATIONS

Term	Description
A&M	Approach and Methodology
DIT(S)	Income Tax Office
DIT(S)	Directorate of Income Tax (Systems)
CCN	Change Control Notice
CV	Curriculum Vitae
CMC	Central Monitoring Center
EMD	Earnest Money Deposit
FAT	Final Acceptance Test
NMS	Network Management System
IP	Internet protocol
RFP	Request for proposal
SI	System integrator
ToR	Terms of Reference
DIT(S)	DIT(S)

Contents

1. Key Events and Dates:

S. No	Items of information	Details
1.	Name of the Employer	President of India acting through Additional Director General (Systems)-2
2.	Name of the contact person for any clarification	Name: Shri. Alok Srivastava, JD(S) Address: 6th Floor, Room No. 6003, Aayakar Bhawan, Vaishali, Ghaziabad (UP-201010). Tel No. +91 0120-2770050 E-mail: aloksrivastava@incometax.gov.in
3.	Tender Inviting authority	Directorate of Income Tax (Systems), Income Tax Department, Ministry of Finance, Government of India
4.	Job Requirement	Selection of System Integrator for “CCTV Surveillance, Access Control & Security Scanning system”
5.	Publication of the RFP Notification	31/05/2019
6.	Building/Site Inspection by the prospective bidders	07/06/2019 to 17/06/2019
7.	Last date of receiving written queries/clarifications by bidders	16:00 Hours on 24/06/2019

S. No	Items of information	Details
8.	Date of response to bidder queries	05/07/2019
9.	Time, date & venue of the pre-bid conference	11:00 Hours on 12/07/2019 11th floor, Conference Hall, Aayakar Bhawan, Vaishali, Ghaziabad-201010
10.	Last date and time for submission of bids	Upto 15:00 Hours on 23/07/2019
11.	Date and Time of opening of Technical Bids	24/07/2019, 16:00 Hours
12.	Date and time for the opening of Financial Bids	07/08/2019, 17:00 Hours
13.	Date till which the RFP response should be valid	180 days from the last date of submission of bids
14.	Bid Submission	Bid submission must be made online at https://eprocure.gov.in/eprocure/app and verified downloaded copy of bid documents to be submitted at 6th Floor, Room No. 6003, Aayakar Bhawan, Vaishali, Ghaziabad (UP-201010).
15.	Bid security/Earnest Money Deposit amount payable	Rs. 10,00,000/-

2. Master Services Agreement

THIS MASTER SERVICE AGREEMENT ("Agreement") is made on this the <***> day of <***> 20… at <***>, India.

BETWEEN

--- having its office at -- India hereinafter referred to as **'DIT(S)',** which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>**,** a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as **'the System Integrator/SI'** which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the '**Parties**' and individually as a '**Party**'.

WHEREAS:

1. DIT(S) is desirous for Implementation and Operations Management of "CCTV Surveillance, Access Control & Security Scanning system".
2. In furtherance of the same, DIT(S) undertook the selection of a suitable System Integrator through a limited tendering process for implementing the Project and in this behalf issued Request for Proposal (RFP) dated <***>.
3. The successful bidder has been selected as the System Integrator on the basis of the bid response set out as Annexure of this Agreement, to undertake the Project of the development and implementation of the solution, its roll out and sustained operations.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

Definitions, Interpretation and General Obligations & Conditions

2.1 Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the meanings set out in Schedule I.

2.2 Interpretation

In this Agreement, unless otherwise specified:

i) references to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and Annexures to this Agreement;

ii) use of any gender includes the other genders;

iii) references to a ‘company’ shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

iv) references to a ‘person’ shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

v) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;

vi) any reference to a ‘day’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;

vii) references to a ‘Business day’ shall be construed as a reference to a day (other than Saturday, Sunday and other gazetted holidays) on which DIT(S) is generally open for business

viii) references to times are to Indian Standard Time;

ix) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

x) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

xi) System Integrator (SI) has been used for the same entity i.e. bidder selected for the project.

2.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

2.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

i) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

ii) as between the provisions of this Agreement and the Schedules/Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and

iii) as between any value written in numerals and that in words, the value in words shall prevail.

2.5 Priority of Documents

This Agreement, including its Schedules and Annexures, represents the entire agreement between the Parties as noted in this Clause. If in the event of a dispute as to the interpretation or meaning of this Agreement it should be necessary for the Parties to refer to documents forming part of the bidding process leading to this Agreement, then such documents shall be relied upon and interpreted in the following descending order of priority:

i) This Agreement along with NDA agreement, Schedules and Annexures;

ii) Request for Proposal and Addendum / Corrigendum to the Request for Proposal (if any).

For the avoidance of doubt, it is expressly clarified that in the event of a conflict between this Agreement, Annexures / Schedules or the contents of the RFP, the terms of this Agreement shall prevail over the Annexures / Schedules and Annexures / Schedules shall prevail over the contents and specifications of the RFP.

2.6 Scope of the Project

DIT(S) has decided to engage a System Integrator who will help in maintaining the security and provide 24 hours surveillance at Aayakar Bhawan, Vaishali. The functions and tasks to be performed by SI have been described in detail further in this Volume of the RFP under the head Scope of Project.

2.7 Term and Duration of the Agreement

This Agreement shall come into effect from date of acceptance of Letter of Intent by the System Integrator (hereinafter the “Effective Date”) and shall, unless terminated earlier in accordance with its terms, expire on the date on which this Agreement expires, which shall be a period of five years from ‘Go-Live’ of the Project and any extended period as notified by DIT(S). In the case of such extension of contract beyond the stipulated period, the warranties, Performance Bank Guarantee, insurance etc. shall be extended for equivalent period.

2.8 System Integrator to obtain his own Information

i) The System Integrator in fixing his rate shall for all purpose whatsoever is deemed to have him independently obtained all necessary information for the purpose of preparing his tender. The correctness of the details, given in the RFP Document to help the System Integrator to make up the tender, is not guaranteed.

ii) The System Integrator shall be deemed to have examined the contract documents, to have generally obtained his own information in all matters whatsoever that might affect carrying out the works at the scheduled rates and to have satisfied himself to the sufficiency of his tender.

iii) Any error in description or quantity or any other aspect in scheduled rates or omissions there from shall not vitiate the contract or release the System Integrator from executing the work comprised in the contract according to drawings and specifications at the scheduled rates. He is deemed to know the scope, nature and magnitude of the work and the requirements of materials and labour and the type of work involved etc.; and as to what all he has to do to complete the works in accordance with the contract documents whatever be the defects, omissions or errors that may be found in the Contract Documents.

iv) The System Integrator is deemed to have acquainted as to its liability for payment of Government taxes, customs duty and other charges.

v) Sites for disposal of surplus materials the available accommodation as to whatever required as depots and such other buildings as may be necessary for executing and completing the works, to have made local independent enquiries as to the subsoil, sub-soil water and variations thereof, storms, prevailing winds, climatic conditions and all other similar matters affecting these works.

vi) Any neglect or failure on the part of the System Integrator in obtaining necessary and reliable information upon the foregoing or any other matters affecting the contract shall not relieve him from any risks or liabilities or the entire responsibility from completion of the works at the schedule rates and time in strict accordance with the contract documents.

vii) No verbal agreement or inference from conversation with any officer or employee of DIT(S) either before or after the execution of the Contract Agreement shall in any way affect or modify any of the terms of obligations herein contained.

2.9 Force Majeure

Any delay in or failure of performance of either party hereto shall not constitute default hereunder or give to any claims for damages if and to the extent such delays or failure of performance is caused by occurrence such as Acts of God or the public enemy; expropriation or confiscation of facilities by Government authorities, compliance with any order or request of any Governmental authority, acts of way, rebellion or sabotage or damage resulting there from, fires, floods, explosion, riots or illegal strikes. The Contractor shall keep record of the circumstances referred to above which are responsible for causing delays in the completion of work and bring these to the notice of the DIT(S).

2.10 Right of Owner to Forfeit Security Deposit

Whenever any claim against the System Integrator for the payment of a sum of money arises out of or under the Contract including deficiency in performance of services, Owner shall be entitled to recover such sum by appropriating in part or whole, the security deposit of the System Integrator forming whole or part of such security deposit. In the event of the security deposit being insufficient or if no security deposit has been taken from the System Integrator, then the balance or the total sum recoverable, as the case may be, shall be deducted from any sum then due or which at any time thereafter may become due to the System Integrator under this or any other contract with Owner and should this be not sufficient to cover the recoverable amount the System Integrator shall pay to Owner on demand the balance remaining due.

2.11 Action When Whole of Security Deposit is Forfeited

i) In any case in which under any clause of this contract the DIT(S) shall have forfeited the whole of his security deposit (whether paid in one sum or deducted by instalments) or the System Integrator has committed a breach of any of the terms contained in this contract, the DIT(S) shall have power to adopt any of the following courses as they deem best suited to its interest:

a. To rescind the contract (of which rescission notice in writing to the System Integrator under the hand of the DIT(S) shall be conclusive evidence) in which case the security deposit of the System Integrator shall stand forfeited and be absolutely at the disposal of DIT(S).

b. To measure up the work of the System Integrator and to take such part thereof as shall be unexecuted out of his hands and to give it to another System Integrator to complete, in which case any expenses which may be incurred in excess of the sum which would have been paid to the original System Integrator, the whole work had been executed by him (of the amount of which excess the certificate in writing of the DIT(S) shall be final and conclusive) shall be borne and paid by the original System Integrator and may be deducted from any money due to him by DIT(S) under the contract or otherwise or from his security deposit or from the proceeds of sale thereof, or a sufficient part thereof.

ii) In the event of any of the above courses being adopted by DIT(S), the System Integrator shall have no claim to compensation for any loss sustained by him by reason of his having purchased or procured any materials or entered into any agreements or made any advances on account of or with a view to the execution of the work or the performance of the contract. And in case the contract shall be rescinded under the provision aforesaid the System Integrator shall not be entitled to recover or be paid any sum for any work therefore actually performed under this contract unless and until the DIT(S) will certify in writing the performance of such work, and the value payable in respect thereof and he shall only be entitled to be paid the value so certified.

iii) In any case in which any of the powers conferred upon DIT(S) by clause 2.11 thereof shall have become exercisable and the same had not been exercised, the non-exercise thereof shall not constitute a Waiver of any of the conditions hereof and such powers shall notwithstanding be exercisable in the event of any future case of default by the System Integrator for which by any clause or clauses hereof he is declared liable to pay compensation amounting to the whole of his security deposit, and liability of the System Integrator for past and future compensation shall remain unaffected.

2.12 DIT(S) Not Bound by Personal Representation

The System Integrator shall not be entitled to any increase on the schedule of rates or any other right or claim whatsoever by reason of any representation, explanation or statement on alleged representation, promise or guarantees given or alleged to have been given to him by any person.

2.13 Members of DIT(S) Not Individually Liable

No Director, or Officer, official or employee of DIT(S) shall in any way be personally bound or liable for the acts or obligations of DIT(S) under the contract or answerable for any default or omission in the observance or performance of any of the acts, matters, or things which are herein contained.

2.14 System Integrator's Subordinate Staff and Their Conduct

i) The System Integrator after the award of the work should name the person responsible for the work, to whom equipment and materials, if any, will be issued and to whom all site instructions and notices can be issued. He should have necessary Power of Attorney which shall be deposited with the DIT(S) in original.

ii) **System Integrator's staff strength:** The System Integrator shall provide, to the satisfaction of the DIT(S) sufficient and qualified staff to superintend the execution of the works, competent sub-agents, Engineering assistants, foremen and leading hands including those specially qualified by previous experience to supervise the types of works comprised in the contract in such a manner as will ensure work of the best quality, expeditious working and proper supervision shall be employed, and whenever in the opinion of the DIT(S) this is not the case, additional and properly qualified supervisory staff shall be employed by the System Integrator without additional charge on account thereof. The System Integrator shall ensure to the satisfaction of DIT(S) that sub-System Integrators, if any, shall provide competent and efficient supervision over the work entrusted to them. Where so required, the System Integrator shall furnish an organization chart as well as full details of staff.

iii) **Conduct of System Integrator's Staff:** The System Integrator shall be responsible for the proper behaviour of all the staff, foremen, workmen and others, and shall exercise a proper degree of control over them and in particular and without prejudice to the said generality, the System Integrator shall be bound to prohibit and prevent any employees from trespassing or acting in any way detrimental or prejudicial to the interests of the community or of the proprietor or occupiers of land and properties in the neighbourhood and in the event of such employee so trespassing, the System Integrator shall be responsible therefore and relieve DIT(S) of all consequent claims or actions for damages or injury or any other grounds whatsoever. The decision of the DIT(S) upon any matter arising under this clause shall be final.

iv) If and whenever any of the System Integrator's or sub-System Integrator's agents, sub-agents, assistants, foremen or others employees shall in the opinion of DIT(S) be guilty of any misconduct or be incompetent or insufficiently qualified or negligent in the performance of their duties or that in the opinion of the DIT(S), it is undesirable for administrative or any other reason for such person or persons to be employed in the works, the System Integrator if so directed by the DIT(S), shall at once remove such person or persons from employment thereon. Any person or persons so removed from the works shall not again be employed in connection with the works without the written permission of the DIT(S). Any person so removed from the works shall be immediately replaced at the expense of the System Integrator by a qualified and competent substitute. Should the System Integrator be requested to repatriate any person removed from the works, he shall do so and shall bear all costs in connection herewith.

v) If and when required by DIT(S), all System Integrators personnel entering upon the premises shall be properly identified by badges displaying their name & designation all times on the premises of the DIT(S) and all work sites.

2.15 Power of Entry

i) If the System Integrator does not commence the work in the manner previously described in the contract documents or if he shall at any time in the opinion of the DIT(S);

a. Fails to carry on the works in conformity with the contract documents, or

b. Fails to carry on the works in accordance with the time schedule, or

c. Substantially suspend work or the works for a period of fourteen days without authority from the DIT(S), or

d. Fails to carry on and execute the works to the satisfaction of the DIT(S), or

e. Fails to supply sufficient or suitable constructional plant, temporary works, labour, materials or things, or

f. Commit or suffer or permit any other breach of any of the provisions of contract on his part to be performed or observed or persist in any of the above mentioned breaches of the contract for fourteen days, after notice in writing shall have been given to the System Integrator by the DIT(S) requiring such breach to be remedied, or

g. If the System Integrator abandon the works, or

h. If the System Integrator during the continuance of the contract become bankrupt, make any arrangement or composition with his creditors or permit any execution to be levied or go into liquidation whether compulsory, or voluntary (not being merely a voluntary liquidation for the purpose of amalgamation or reconstruction).

ii) Then, in any such case, the DIT(S) shall have the power to enter upon the works and take possession thereof and of the materials, temporary works, constructional plant, and stock thereon, and to revoke the System Integrator's license to use the same, and to complete the works by his agents, other System Integrators, or workmen, or to relent the same upon any terms and to such other person, firm or corporation as the DIT(S) in his absolute discretion may think proper to employ, and for the purpose aforesaid to use or authorize the use of any materials, temporary works, considered plant, and stock as aforesaid, without making payment or allowance to the System Integrator for the said materials other than such as may be certified in writing by the DIT(S) to be reasonable, and without making any payment or allowance to the System Integrator for the use of the said temporary works, constructional plant and stock or being liable for any loss for damage there to, and if the DIT(S) shall by reason of his taking possession of the works or of the works being completed by other System Integrator (due account being taken of any such extra work or works which may be omitted) then the amount of such excess as Integrator and DIT(S) shall have power to sell in such manner and for such price as DIT(S) may think fit and or any of the constructional plant, materials etc.; construction by or belonging to and to recoup and retain the said deficiency or any part thereof out of the proceed of the sale.

2.16 Notices

Any notice hereunder may be served on the System Integrator or his duly authorized representative at the job site or may be served by registered post, speed post, e-mail direct to the address/ email-id furnished by the System Integrator. Proof of issue by DIT(S) of any such notice would be conclusive of the System Integrator having been duly informed of all contents therein.

2.17 Rights of Various Interests

Wherever the work being done by any department of the DIT(S) or by other System Integrators employed by the DIT(S) the respective rights of the various interests involved shall be determined by the DIT(S) to secure the completion of the various portions of the work in general harmony.

2.18 Qualified and Experienced Personnel

The System Integrator shall ensure at all times that it has sufficient, suitable and qualified personnel with requisite experience to undertake the responsibilities imposed upon the System Integrator under the Contract.

2.19 Termination of Contract

i) DIT(S), shall, at any time, be entitled to determine and terminate the contract, if in its opinion the cessation of the work becomes necessary owing to paucity of funds, change in scheme or from any other cause, whatsoever, in which case the cost of approved materials at the site at current market rates as verified and approved by DIT(S) and of the value of the work done to date by the System Integrator shall be paid for in full at the rates specified in the contract. A notice in writing from the DIT(S) to the System Integrator of such determination and termination and the reason therefore shall be the conclusive proof of the fact that the contract has been so determined and terminated by DIT(S).

ii) Should the contract be determined under sub-clause (i) of this clause and the System Integrator claims payments to compensate expenditure incurred by him in the expectation completing the whole of the work, the DIT(S) shall consider and admit such claims, as are deemed fair and reasonable and are supported by vouchers to his satisfaction. The decision of DIT(S) on the necessity and proprietary of any such expenditure shall be final and conclusive and be binding on the System Integrator.

2.20 Mutual Rescission

No mutual rescission of this contract or the mutual rescission of any obligation of either party hereto, shall be binding upon the other party unless such mutual rescission is reduced to writing and signed by both parties hereto.

2.21 Bankruptcy

If a petition of bankruptcy is filed by or against the System Integrator, DIT(S) may, at its opinion, and within sixty days of the filing of such petition cancel this contract and agreement provisions contained in Clause 2.19 (a) above shall apply in such a case.

2.22 Patents, Royalties & Lien

i) The System Integrator, if licensed under and patent covering equipment, machinery, materials compositions of matter to be used or supplied or methods and process to be practiced or employed in the performance of this contract, agrees to pay all royalties and license fees which may be due with respect thereto. If any equipment, machinery, materials, composition of matters to be used or supplied or methods and processes to be practised or employed in the performance of this contract is covered by a patent, then the System Integrator, before supplying or using the equipment, machinery, materials, composition, methods or process shall obtain such licenses and pay such royalties and license fees as may be necessary for performances of this contract. In the event the System Integrator fails to pay any such royalty or obtain any such license any suit for infringement of such patents which is brought against the System Integrator or DIT(S) as a result of such failure will be defended by the System Integrator at his own expense and the System Integrator will pay any damage and costs awarded in such suit. The System Integrator shall promptly notify DIT(S) if the System Integrator has acquired knowledge of any plant under which a suit for infringement could be reasonably brought because of the use by DIT(S) of any equipment, machinery, materials, composition, process, methods to the supplied hereunder.

ii) The System Integrator agrees to and does hereby grant to DIT(S) together with the right to extend the same to any of the subsidiaries of DIT(S) as irrevocably, royalty- free license to use in any country; any invention made by the System Integrator or his employee in or as a result of the performance of the work under the contract.

iii) DIT(S) shall indemnify and save harmless the System Integrator from any loss of account of claims against System Integrator for the contributory infringement of patent rights arising out and based upon the claim the use by DIT(S) of the process included in the design prepared by DIT(S) and used in the operation of the plant infringes on any patent rights. With System Integrator pursuant to the provisions of the relevant clause hereof the System Integrator shall obtain from the sub-System Integrator an undertaking to provide DIT(S) with the same patent protection that System Integrator is required to provide under the provisions of this clause.

iv) All drawings, blue prints, tracings, reproducible, models, plans, specifications and copies thereof furnished by DIT(S) as well as all drawings, tracings, reproducible, plans, specifications, design, calculations etc. prepared by the System Integrator for the purposes of execution of work covered in or connected with this contract shall be the property of DIT(S) and shall not be used for any other work but are to be delivered to DIT(S) at the completion of the contract.

v) Where so desired by DIT(S), the System Integrator agrees to respect the secrecy of any documents, drawings etc. issued to him for the execution of this contract, and restrict access to such documents, drawings etc. to the minimum and further, the System Integrator agrees to execute an individual SECRECY agreement from each or any person employed by the System Integrator having access to such documents, drawings etc. In any event the System Integrator shall not issue drawings and documents to any other agency or individual without the written approval by DIT(S).

Lien

i) If, at any time, there should be evidence of any lien or claim for which DIT(S) might have become liable and which is chargeable to the System Integrator, DIT(S) shall have the right to retain out of any payment then due or thereafter becomes due an amount sufficient to completely indemnify DIT(S) against such lien or claim and if such lien or claim be valid DIT(S) may pay and discharge the same and deduct the amount so paid from any money which may be or may become due and payable to the System Integrator. If any lien or claim remaining unsatisfied after all payments are made, the System Integrator shall refund or pay to DIT(S) all moneys that the latter may be compelled to pay in-discharging such lien or claim including all costs and reasonable expenses.

ii) The final payment shall not become due until the System Integrator delivers to the DIT(S) as complete release or waiver of all liens arising or which may arise out of this agreement or receipts in full or certification by the System Integrator in a form approved by DIT(S) that all invoices for labour, materials and services have been paid in lien thereof and if required by the DIT(S) in any case, an affidavit that so far as the System Integrator has knowledge or information the releases and receipts include all the labour and material for which a lien could be filled.

iii) System Integrator will indemnify and hold DIT(S) harmless for a period of two years after the issue of final certificate from all liens and other encumbrances against DIT(S) on account of debts or claims alleged to be due from the System Integrator or his sub-System Integrator to any person including sub-System Integrators and on behalf of DIT(S) will defend at his own expenses any claim or litigation in connection therewith System Integrator shall defend or contest at his own expense any fresh claim or litigation brought against DIT(S) or the System Integrator by person including even after the expiry of two years from the date of issue of final certificate.

iv) System Integrator shall indemnify and save DIT(S) from and against all actions, suits proceedings, losses, costs damages, charges claims and demands of every nature and description brought or recovered against DIT(S) by reason of any act or omission of the System Integrator, his agents or employees in the execution of the work or in regarding the same. All sums payable by way of compensation under any of these conditions shall be considered as reasonable compensation to be applied to the use of DIT(S) without references to the actual loss or damage sustained and whether or not any damage shall have been sustained.

2.23 Publicity

i) System Integrator shall not disclose details of the work to any person or persons except those engaged in its performance, and only to the extent required for the particular portion of the work being done.

ii) System Integrator will not give any items concerning details of the work to the press or a news dissemination agency without prior written approval from DIT(S). System Integrator shall not take any picture on site without specified written approval of DIT(S) representative.

2.24 Operation of Contract

i) Governing Laws &Jurisdiction: The terms and provisions of this Contract shall be governed and interpreted in accordance with the laws of India in force and is subjected to and referred to the court of law located at New Delhi which shall have exclusive jurisdiction. Regardless of the place of contracting, place of performance or otherwise, this agreement, and all amendments modifications, alterations, or supplements, thereto shall be governed by the law of India and particularly the State of Uttar Pradesh.

ii) Non-waiver of Defaults: Any failure by DIT(S) or System Integrator at any time, or from time to time, to enforce or require the strict keeping and performance of any of the terms or conditions of this Agreement, or to exercise a right hereunder, shall not constitute a waiver of such terms, conditions, or rights and shall not affect or impair same, or the right of DIT(S) or System Integrator, as the case may be, at any time to avail itself of same.

2.25 Schedule of Rates to be Inclusive

i) Schedule of Rates shall be deemed to include and cover all costs, expenses and liabilities of every description and all risks of every kind to be taken in executing, completing and handing over the work to DIT(S) by the System Integrator. The System Integrator shall be deemed to have known the nature, scope, magnitude and the extent of the works and materials required, though the contract documents may not fully and precisely furnish them. He shall make such provision in the Schedule of Rates as he may consider necessary to cover the cost of such item of work and materials as may be reasonable and necessary to complete the works. The opinion of the DIT(S) as to the items of work which are necessary and reasonable for completion of work shall be final and binding on the System Integrator, although the same may not be shown on or described specifically in contract documents.

ii) Generality of this present provision shall not be deemed to cut down or limit in any way because in certain cases it may and in other cases it may not be expressly stated that the System Integrator shall do or perform a work or supply articles or perform services at his own cost or without additional payment or without extra charges or words to the same effect or that it may be stated or not stated that the same are included in and covered by the Schedule of Rates.

2.26 Schedule of Rate to Cover Equipment, Materials, Labour Etc.

Without in any way limiting the provisions of the preceding sub-clause the Schedule of Rates shall be deemed to include and cover the cost of all equipment, materials, labour, insurance, fuel, stores and appliances to be supplied by the System Integrator and all other matters in connection with each item in every respect maintained and as shown or described in the contract documents or as may be ordered in writing during the continuance of the contract.

2.27 Schedule of Rates to Cover Royalties, Rent & Claims

The Schedule of Rates shall be deemed to include and cover cost of all royalties and fees for all articles, protected by letters, patent or otherwise incorporated or used in connection with the works, also all royalties, rents and other payments in connection with obtaining materials of whatsoever kind for the works and shall include an indemnity of DIT(S) which the System Integrator hereby gives against all actions, proceedings, claims, damages, costs and expenses arising from the incorporation or the use of the works of any such articles, processes or materials. Octroi or other Municipal or local Board charge, if levied on materials to be brought to site and removed from site for use on work or after completion of the work, shall be borne by System Integrator.

2.28 Schedule of Rates to Cover Taxes & Duties

No exemption or reduction of customs duties, GST, quay or any part duties, transport carriages, stamp duties of Central or State Government or other body including one company or dues, taxes or charges (from or of any other body including the company), whatsoever will be granted or obtained all of which expenses shall be deemed to be included in and covered by the Schedule of Rates. The System Integrator shall also obtain and pay for all permits, or other privileges necessary to complete work.

2.29 Schedule of Rates to Cover Risks of Delay

The Schedule of Rates shall be deemed to include and cover the risk of all possibilities of delay and interference with the System Integrator’s conduct of the works which occur from any cause including orders of DIT(S) in the exercise of his powers and on account of extension of time granted due to various reasons and for all other possible or probable causes of delay.

Performance of Work

2.30 Execution of Works

i) All the works shall be executed in strict conformity with the provisions of the contract documents and with such explanatory detailed drawings, specifications and instructions as may be furnished from time to time to the System Integrator by the DIT(S) whether mentioned in the contract or not. The System Integrator shall be responsible for ensuring that works throughout are executed in the most substantial proper workman like manner with the quality of material and workmanship in strict accordance with the specifications and to the entire satisfaction of the DIT(S).Wherever it is mentioned in the specifications that the System Integrator shall perform certain work or provide certain facilities/ materials, it is understood that the System Integrator shall do so at his cost.

2.31 Police Verification

The System Integrator shall ensure that only those personnel are deputed for the services under the contract whose police verification has been done and nothing adverse has been found.

2.32 Articles of Value Found

All gold, silver and other minerals of any description and all precious stones, coins, treasure, relics, antiquities and other similar things which shall be found in, under or upon the site shall be the property of DIT(S) and the System Integrator shall only preserve the same to the satisfaction of the DIT(S) and shall from time to time deliver the same to such person or persons indicated by the DIT(S).

2.33 Discrepancies between Instructions

Should any discrepancy occur between the various instructions furnished to the System Integrator, his agents or staff or any doubt arise as to the meaning of any such instructions or should there be any misunderstanding between the System Integrator's staff and the DIT(S)'s staff, the System Integrator shall refer the matter immediately in writing to the DIT(S) whose decision thereon shall be final and conclusive and no claim for losses alleged to have been caused by such discrepancies between instructions, doubts, or misunderstanding shall in any event be admissible.

2.34 Action & Compensation in Case of Bad Work

If it shall appear to the DIT(S) that any work has been executed with unsound, imperfect or unskilled workmanship, or with materials of any inferior description, or that any materials or articles provided by the System Integrator for the execution of the work are unsound, or of a quality inferior to the contracted for, or otherwise not in accordance with the contract, the System Integrator shall on demand in writing from the DIT(S) or his authorized representative specifying the work, materials or articles complained of, notwithstanding that the same may have been inadvertently passed, certified and paid for, forthwith rectify or remove and reconstruct the work so specified and provide other proper and suitable materials or articles at his own charge and cost, and in the event of failure to do so within a period to be specified by the DIT(S) in his demand aforesaid, the System Integrator shall be liable to pay compensation at the rate of half per cent of the estimated cost of the whole work for the value of the whole work, while his failure to do so shall continue and in the case of any such failure the DIT(S) may on expiry of notice period rectify or remove, and re-execute the work or remove and replace with others, the materials or articles complained of as the case may be at the risk and expense in all respect of the System Integrator. The decision of the DIT(S) as to any question arising under this clause shall be final and conclusive.

2.35 Suspension of Works

The System Integrator shall if ordered in writing by the DIT(S), or his representative, temporarily suspend the works or any part thereof for such period and such time as so ordered and shall not after receiving such written orders, proceed with the work therein ordered to be suspended until he shall have received a written order to proceed therewith, the System Integrator shall not be entitled to claim compensation for any loss or damage sustained by him by reason of this temporary suspension of the works aforesaid. An extension of time for completion, corresponding with the delay caused by any such suspension of the works as aforesaid will be granted to the System Integrator should he apply for the same provided that the suspension was not consequent to any default or failure on the part of the System Integrator.

Procedure for Billing of Work In Progress

2.36 Payment Schedule

Sl. No	Payment Milestone	Deliverables/ Milestone (for marking closure of SI Activity & Task)	Timelines* (T=Date of signing the Contract)	Payments (% of the total project cost)
1.	Hardware and software Delivery	Validation of bills submitted by SI along with acknowledgement from the site officer	T + 2 months	30%
2.	Acceptance	Acceptance Test report by DIT(S) or its nominated agencies	T + 4 months	40%*
3.	Post Go-live Support	Validation of SLA adherence report and Physical Surveillance Compliance Report on a Quarterly basis	Yearly payment of 5% every year (Upto 5years after Go Live)	25%**
4.	Handing Over	Handing over report to DIT(S) or its nominated agencies	60 months after Go live	5%

* This amount shall include the cost of Project Manager.

** This amount shall include the cost of manpower excluding Project Manager.

2.37 Notice of Claims for Additional Payment

Should the System Integrator, consider that he is entitled to any extra-payment or compensation or to make any claims whatsoever in respect of the works he shall forthwith give notice in writing to the DIT(S) that he claims extra payment and/ or compensation. Such notice shall be given to the DIT(S) within ten days, from the ordering of any work or happening of any event upon which the System Integrator basis such claims. Notice shall contain full particulars of the nature of such claims with full details and amount claimed. Failure on the part of the System Integrator to put forward any claim with the necessary particulars as above within the time above specified shall be an absolute waiver thereof. No omission by the DIT(S) to reject any such claim and no delay in dealing therewith shall be a waiver by the DIT(S) of any rights in respect thereof.

2.38 Payment of System Integrator's Bill

i) The bills/invoices along with all supporting document in duplicate shall be submitted to DIT(S) for payment. DIT(S) will make efforts to make payment to the System Integrator within 60 (Sixty) days of receipt of all necessary supporting documents. The penalties shall be imposed on System Integrator as per the penalty criteria specified in SLA.

ii) All payments to and recoveries from the System Integrator shall be rounded off to the nearest rupee. Wherever the amount to be paid/recovered consists of a fraction of a rupee (paise), the amount shall be rounded off to the next higher rupee if the fraction consists of 50 (fifty) paise or more and if the fraction of a rupee is less than 50 (fifty) paise, the same shall be ignored.

iii) Payment due to the System Integrator shall be made by the DIT(S), by Crossed 'Account Payee' cheque or direct bank transfer, if applicable in Directorate.

iv) All payments shall be made in Indian currency.

2.39 Performance/Completion Certificate

i) Application for Performance/Completion Certificate: When the System Integrator fulfils his obligation under the Contract he shall be eligible to apply for performance/completion certificate.

ii) DIT(S) shall issue to the System Integrator the performance/completion certificate within one month after receiving an application in writing from System Integrator after verifying from the completion documents and satisfying himself that the work/service has been completed in accordance with the contract documents.

2.40 Unconditional No Claim Certificate

Unconditional no claim certificate shall be furnished by the System Integrator along with final bill with the intent that the final bill prepared by the System Integrator shall reflect any and all claims whatsoever of the System Integrator against the DIT(S) arising out of or in contract or work performed by the System Integrator.

Taxes and Insurance

2.41 Taxes, Duties, Octroi, etc.

i) The quoted prices shall be deemed to be inclusive of all applicable direct or indirect taxes (central or state or local), rates, duties, charges and levies (central or state or local), except GST. The Income tax at the prevailing rate will be deducted from System Integrator's bills as per Income Tax Act.

ii) Notwithstanding the foregoing, DIT(S) shall not bear any liability in respect of:

a. Personal taxes on the personnel deployed by the System Integrator, his Sub-System Integrator and Agent, etc.

b. The Corporate Taxes, any other taxes on income in respect of System Integrator and his Sub-System Integrator and other Agents, Indian or foreign based.

c. Any other taxes/ duties/ levies.

2.42 Payment of Taxes

The System Integrator shall be fully and exclusively responsible for the payment (and liable for all consequences in the event of default) of any and all taxes, duties, cess, levies, GST, works contract tax etc now or hereafter imposed, increased or modified from time to time in respect of the above job and all contributions and taxes for un-employment compensation, insurance and old age pensions and annuities now or hereafter imposed by any law of the Government/local bodies which are imposed with respect to or covered by the wages, salaries or other compensation paid to the persons employed by the System Integrator. DIT(S) shall have no liability whatsoever concerning the employees/labourers of the System Integrator. The System Integrator shall keep DIT(S) indemnified against all losses or damage or liability arising out of or imposed in the case of employees.

i) System Integrator further agrees to defend, indemnify and hold harmless from any liability or penalty which may be imposed by the Central, State or local authorities by reason of any violation by System Integrator or sub-System Integrator of such laws, regulations or requirements and also from all claims, suits or proceedings that may be brought against DIT(S) arising under growing out of, or by reason of the work provided for by this contract, whether brought by employees of the sub-System Integrator by third parties, or by Central or State Government authority of any administrative sub-division thereof, or other local authorities.

2.43 Insurance

i) The System Integrator shall at his own cost and initiative take out and maintain at all times until the expiry / termination of the Contract, insurance policies in respect of workmen engaged by him for providing services under this Contract, in order to keep himself as well DIT(S) fully indemnified from and against all claims whatsoever including but not limited to those arising out of the provisions contained in Workmen's Compensation Act, 1923. Should the System Integrator fail to take insurance as provided for in the foregoing paragraph, DIT(S) shall be entitled (but without any obligation to do so) to take such insurance at the cost and expense of the System Integrator and without prejudice to any other rights or remedies of DIT(S) in this behalf, to deduct the sum(s) incurred thereof from any amounts due to the System Integrator.

ii) System Integrator shall at his own expenses carry and maintain insurance with reputable insurance companies to the satisfaction of DIT(S) as follows:

(i) Employees State Insurance Act

- The System Integrator agrees to and does hereby accept full and exclusive liability for the compliance with obligations imposed by the Employees State Insurance Act, 1948, as amended from time to time and the System Integrator further agrees to defend, indemnify and hold DIT(S) harmless from any liability or penalty which may be imposed by Central, State or local authority by reason of any asserted violation by System Integrator or sub-System Integrator of the Employees' State Insurance Act. 1948, and its amendments and also from all claims, suits or proceedings that may be brought of by reason of the work provided for by this contract whether brought by employees of the System Integrator, the sub-System Integrator or his employees by third parties or by Central or State Govt. authority or any administrative sub-division thereof, or other local authorities.
- The System Integrator agrees to fill in with Employees' State Insurance Corporation, the Declaration Forms and all forms which may be required in respect of the System Integrator's or sub-System Integrator's employees who are employed in the work provided for or those covered by ESI from time to time under the Agreement. The System Integrator shall deduct and secure the agreement of the sub-System Integrator to deduct the employees' contribution as per the first Schedule of the Employee's State Insurance Act from wages and affix the Employee's Contribution card at wages payment intervals. The System Integrator shall remit and secure the agreement of the sub-System Integrator to remit to the State Bank of India, Employee's State Insurance Corpn. Accounts, the employer's contribution as required by the Act, the term employer being understood as the System Integrator.

- The System Integrator agrees to maintain all cards and records as required under the Act in respect of employees and payments and the System Integrator shall secure the agreement of the sub-System Integrator to maintain such records. Any expenses, incurred for making contributions or maintaining records whether by System Integrator or his sub-System Integrator shall be to the System Integrator's account.

- DIT(S) shall retain such sum as may be necessary from the total contract value until the System Integrator shall furnish satisfactory proof that all contributions as required by the Employees State Insurance Act, 1948, and its amendments from time to time have been paid.

(ii) Workman's Compensation & Employer's Liability Insurance

- Insurance shall be effected for all the System Integrator's employees engaged in the performance of this contract. If any of the work is sublet, the System Integrator shall require the sub-System Integrator to provide Workman's Compensation and employer's responsibility insurance for the latter's employees if such employees are not covered under the System Integrator's Insurance.

(iii) Any other Insurance required under Law or Regulations or by DIT(S).

- System Integrator shall also carry and maintain any and all other insurance which he may be required under any law or regulations from time to time. He shall also carry and maintain any other insurance which may be required by DIT(S).

Labour Laws & Safety Regulations

2.44 Labour Laws

i) No staff below the age of 18 (eighteen) years shall be employed on the work.

ii) The System Integrator shall not pay less than what is provided under law to labourers engaged by him or his sub-System Integrators on this work, for work done other than on item rates basis.

iii) The System Integrator shall at his expenses comply with all labour laws and keep the DIT(S) indemnified in respect thereof.

iv) The System Integrator shall exclusively be liable for non-compliance of the provision of any Acts, laws, rules and regulations having bearing over engagement of labour / workers(s), directly or indirectly for subject work under this Contract.

2.45 System Integrator to Indemnify DIT(S)

i) DIT(S) shall not be liable for any demand or compensation in consequence of any accident or injury to any workmen or other person in the employment of the System Integrator or his sub-System Integrator and System Integrator shall indemnify and keep indemnified DIT(S) against all such damage and compensation and against all claims, damage, proceedings, costs, charges and expenses whatsoever in respect thereof or in relation thereto.

ii) The System Integrator shall indemnify DIT(S) and every member, officer and employee of DIT(S) against any claim, demand, cost and expense whatsoever arising out of any failure by the System Integrator or any of its employees or sub-System Integrators or any of their employees in the performance of the obligations under any law including labour laws, etc. and under the contractual obligations.

iii) The System Integrator hereby undertakes to indemnify DIT(S) against all actions, suits, proceedings, claims, losses, damages etc., which may arise under Minimum Wages Act, Fatal Accident Act, Workmen Compensation Act, Shops & Establishment Act, Family pension & Deposit Linked Insurance scheme or any other Act or statutes not herein specifically mentioned but having any direct or indirect application for the person(s) engaged under this contract by him.

iv) The System Integrator shall defend, indemnify and hold DIT(S) harmless from any liability, which may be imposed by the Central, State or local authorities and also from all claims, suits arising out of or by reason of the work provided by this contract including any liability that may arise out of accident, whether brought by the employees/labourers of the System Integrator or by the third parties or by the Central or State Government authority or any sub-division thereof.

v) DIT(S) shall not be responsible for any claim/compensation that may arise due to damages/injuries/pilferage to the System Integrator's employee(s)/ staff/labourers under any circumstances while an employee(s) /labourer is engaged in the DIT(S)'s/ DIT(S)’s duty under the contract.

2.46 Payment of Claims & Damages

i) Should DIT(S) have to pay any money in respect of such claims or demands as aforesaid the amount so paid and the costs incurred by DIT(S) shall be charged and paid by the System Integrator and the System Integrator shall not be at liberty to dispute or question the right of DIT(S) to make such payments, notwithstanding same may have been made without his consent or authority or in law or otherwise to the contrary.

ii) In every case in which by virtue of the provision of section 12, sub-section (1) of workmen's compensation Act 1923 or other applicable provision of Workman's Compensation Act of any other Act, DIT(S) is obliged to pay compensation to workman employed by the System Integrator in execution of the Works, DIT(S) will recover from the System Integrator the amount of the compensation so paid; and without prejudice to the rights under section 12, sub-section (2) of the said Act, DIT(S) shall be at liberty to recover such amount or any thereof by deducting it from the security deposit or from any sum due to the System Integrator whether under this contract or otherwise. DIT(S) shall not be bound to contest any claim made under section 12, sub-section (1) of the said Act, except on the written request of the System Integrator and upon his giving to DIT(S) full security for all costs for which might become liable in consequence of contesting such claim.

2.47 Employment Liability

i) The System Integrator shall be solely and exclusively responsible for engaging or employing persons for the execution of work and their deployment. The SI shall be fully responsible for the timely payment to all personnel so engaged and deployed. All disputes or differences between the System Integrator and personnel so engaged and deployed shall be settled by him/them. DIT(S) has absolutely no liability whatsoever concerning the personnel so engaged and deployed by the System Integrator. The System Integrator shall indemnify the DIT(S) against all loss or damage or liability arising out of or in the course of his/their employing and/or deploying persons or relations with his/their employees/personnel deployed. The System Integrator shall make regular and full payment of wages and salaries to personnel so engaged and deployed and furnish necessary proof whenever required by the DIT(S). In case of any complaint by any personnel so engaged and deployed by the System Integrator or his sub-System Integrator regarding non-payment of wages, salaries or other dues, DIT(S) reserves the right to make such payments directly to such personnel so engaged and deployed and recover the amount in full from the bills of the System Integrator, and the System Integrator shall not claim any compensation or re-imbursement thereof. The System Integrator shall comply with the Minimum wages Act applicable (U.P. State law) with regard to payment of wages of his employees.

ii) The System Integrator shall deal with and settle all labour dispute related matters without involving the DIT(S).

iii) Personnel so engaged and deployed by the System Integrator shall have no claim ever for any employment under the DIT(S) resulting from or relating to services under the present contract.

2.48 Safety Regulations

i) In respect of all staff, directly or indirectly employed in the work for the performance of System Integrator's part of this agreement, the System Integrator shall at his own expense arrange for all the safety provisions as per safety codes of CPWD, Indian Standards Institution, the Electricity Act, and such other Acts as applicable.

ii) The System Integrator shall observe and abide by all fire and safety regulations.

iii) The System Integrator's staff shall abide by the existing security and safety rules/ regulations/ precautions as per instruction issued to them from time to time by DIT(S). The System Integrator and its staff may also be required to pledge secrecy and non-divulgence of the nature of the work of DIT(S) that may prejudice the interests of DIT(S). System Integrator shall also ensure to engage persons by him whose character and antecedents have been got verified by him and furnish a certificate, in a form and manner prescribed by DIT(S).

iv) The System Integrator undertakes to ensure due and complete compliance with all laws, regulation, rules etc. whether of the Central Government or the State Government or of any other competent authority applicable to the workmen employed or whose services are others wise availed of by the System Integrator whether in connection with the construction work at the site or otherwise. The DIT(S) shall have the right to inspect the records maintained by the System Integrator concerning such workmen from time to time and the System Integrator shall whenever required by the DIT(S) produce such records as the DIT(S) may call upon the System Integrator to produce for the DIT(S) inspection in order to ascertain whether or not the requirements of all such laws, regulations, rules etc. have been complied with by the System Integrator. In the event of any contravention of such laws, regulations, rules etc. coming to light whether as a result of such inspection or to otherwise the DIT(S) shall have the right to require the System Integrator to effect such compliance within such time as the DIT(S) prescribe in that behalf and in the event of the System Integrator failing to effect such compliance within the time prescribed by the DIT(S) then the DIT(S) shall without prejudice to his other rights be entitled to withhold from the amount payable to the System Integrator any amount payable to the workmen under any such laws, regulations or rules and to make payment thereof to the workmen. The DIT(S) shall also have in that event the right to terminate the contract with immediate effect and to exercise powers reserved to the DIT(S) under the contract as a result of termination.

2.49 Arbitration

i) In event of any dispute or difference between the parties hereto, such disputes or differences shall be resolved amicably by mutual consultation. If such resolution is not possible, then the unresolved dispute or difference shall be referred to arbitration of the sole arbitrator to be appointed by the Secretary, Ministry of Finance on the recommendation of the Secretary, Department of Legal affairs ("Law secretary"), Government of India. The Provisions of Arbitration and Conciliation Act, 1996 (No. 26 of 1996) shall be applicable to the arbitration. The venue of such arbitration shall be at Delhi or any other place, as may be decided by the arbitrator. The language of arbitration proceedings shall be English. The arbitrator shall make a reasoned award (the "Award"), which shall be final and binding on the parties." The cost of the arbitration shall be shared equally by the parties to the agreement. However, expenses incurred by each party in connection with the preparation, presentation shall be borne the party itself.

ii) Pending the submission of and /or decision on a dispute, difference or claim or until the arbitral award is published: the Parties shall continue to perform all of their obligations under this Agreement without prejudice to a final adjustment in accordance with such award.

Safety Code – General

2.50 General

System Integrator shall adhere to safe work practice and guard against hazardous and unsafe working conditions and shall comply with safety rules as set forth herein.

2.51 First Aid & Industrial Injuries

i) System Integrator shall maintain First-Aid facilities for his employees and those of his sub-System Integrators.

ii) System Integrator shall make outside arrangements for ambulance service and for the treatment of industrial injuries. Names of those providing these services shall be furnished to DIT(S) prior to start of work, and their telephone numbers shall be prominently posted in System Integrator's office.

iii) All critical industrial injuries shall be reported promptly to the DIT(S) as also a copy of System Integrator's report covering each personal injury requiring the attention of a Physician shall be furnished.

2.52 General Rules

No person shall carry any photographic films, inflammable material within the building premises.

2.53 Demolition

Before any demolition work is commenced and also during the process of the work

i) All roads and open areas adjacent to the work site shall either be closed or suitably protected.

ii) No Electric cable or apparatus which is liable to be a source of danger shall remain electrically charged.

iii) All practical steps shall be taken to prevent danger to persons employed from risk of fire or explosion or flooding. No floor, roof or other part of the building shall be so over loaded with debris or materials as to render it unsafe.

2.54 Safety Equipment

i) All necessary personal safety equipment as considered adequate by the DIT(S), should be kept available for the use of the persons employed on the site and maintained in a condition suitable for immediate use, and the System Integrator should take adequate steps to ensure proper used of equipment by those concerned.

ii) Workers employed on mixing asphaltic materials, cement and lime mortars shall be provided with protective footwear and protective gloves.

iii) Those engaged in white washing and mixing or stacking of cement bags or any materials which are injurious to the eyes shall be provided with protective goggles.

iv) Those engaged in welding and cutting works shall be provided with protective face and eye-shields, hand gloves etc.

v) Stone breakers shall be provided with protective goggles and protective clothing and seated at sufficiently safe intervals.

vi) When workers are employed in sewers and manholes, which are in use, the System Integrator shall ensure that the manholes covers are opened and are ventilated at least for an hour before the workers are allowed to get into the manholes, and the manholes so opened shall be cordoned off with suitable railing and provided with warning signals or boards to prevent accident to the public.

2.55 Risky Places

When the work is done near any place where there is a risk of drawing, all necessary safety equipment should be provided and kept ready for use and all necessary steps taken for prompt rescue of any person in danger and adequate provision should be made for prompt first-aid treatment of all injuries likely to be sustained during the course of the work.

2.56 Hoisting Equipment

i) Use of hoisting machine and tackle including their attachments, anchorage and supports shall conform to the following standard conditions:

a. These shall be of good mechanical construction, sound materials and adequate strength and free from patent defect and shall be kept in good repair and in good working order.

b. Every rope used in hoisting or lowering materials or as a means of suspension shall be of durable quality and adequate strength and free from patent defects.

ii) Every crane driver or hoisting appliance operator shall be properly qualified and no person under the age of 21 years should be in charge of any hoisting machine including any scaffolding winch or give signals to the Operator.

iii) In case of every hoisting machine and of every chain ring hook, shackle, swivel and pulley block used in hoisting or lowering or as means of suspension, the safe working load shall be ascertained by adequate means. Every hoisting machine and all gear referred to above shall be plainly marked with the safe working load and the conditions under which it is applicable shall be clearly indicated. No part of any machine or any gear referred to above in this paragraph shall be loaded beyond the safe working load except for the purpose of testing.

2.57 Electrical Equipment

Motors, Gearing, Transmission, Electric Wiring and other dangerous parts of hoisting appliance should be provided with efficient safe-guards. Hoisting appliances should be provided with such means as will reduce to the minimum risk of accidental descent of the load. Adequate precaution should be taken to reduce to the minimum the risk of any part of a suspended load becoming accidentally displaced. When workers are employed on electrical installations which are already energized, insulating mats wearing apparels, such as gloves, sleeves and boots and insulated tools as may be necessary should be provided. The workers shall not wear any rings, watches and carry keys or other materials which are good conductors of electricity.

3. Schedule I

(i) “Agreement” means this Master Services Agreement, Non-Disclosure Agreement together with all Articles, Annexures, Schedules and the contents and specifications of the RFP;

(ii) “Applicable Law(s)” means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;

(iii) “Business Hours” shall mean the working time for DIT(S) users which is 9:30 AM to 6:00 PM.

(iv) “Effective Date” shall have the same meaning ascribed to it in Clause 2.7

(v) “Force Majeure” shall have the same meaning ascribed to it in Clause 2.9

(vi) “Parties” means DIT(S) and System Integrator for the purposes of this Agreement and “Party” shall be interpreted accordingly;

(vii) “Scheduled Operation Time” means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the monitoring center and DIT(S) will be 24 X 7. The total operation time means when the manpower is required at DIT(S) and Monitoring Centre.

(viii) “Performance Bank Guarantee” means the guarantee provided by a Nationalized / Scheduled Bank in favour of the System Integrator. The amount of Performance Bank Guarantee shall be 10% of the estimated contract value specified in section 6.5 of Volume – I of the RFP. This Performance Bank Guarantee shall be valid from the date of acceptance of the Letter of Intent and shall continue till sixty days after the completion of all contractual liabilities including warranty obligations and defect liability period as per CVC guidelines;

(ix) “Availability” shall mean the time for which the services and facilities offered by the SI are available for conducting operations from the equipment installed at the DIT(S) and it is defined as:

(x) Uptime shall be calculated as {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} x 100%

(xi) “Downtime” means accumulated time during which the system is inoperable within the Scheduled Operation Time but outside the scheduled maintenance time and measured from the time the DIT(S) (office) log a call for the failure or the failure is known to the SI from the availability measurement tools to the time when the system is returned to proper operation.

(xii) The SLA metrics provided specifies performance parameters as baseline performance, lower performance and breach. All SLA calculations will be done on quarterly basis. The SLA also specifies the penalties for lower performance and breach conditions.

(xiii) The yearly payment shall be made after deducting the penalty as mentioned above. DIT(S) or its nominated project management agency will validate the SLA reports submitted by the vendor for payment clearance.

(xiv) The SLA parameters shall be measured on the basis of individual SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the SI and audited by DIT(S) or its nominated project management agency for accuracy and reliability.

(xv) DIT(S) shall be entitled to, at its discretion, to extend the time period for implementation and acceptance of the overall solution of the project, for any delay or defects or non-performance not directly attributable to the SI.

(xvi) Any delay or defect not directly attributable to the System Integrator, shall not amount to breach or Material breach by the System Integrator of this Agreement. DIT(S) shall be entitled to, at its discretion, to extend the time period for implementation and acceptance of the Total Solution of the Project, for any delay or defects or non-performance not directly attributable to the Partner.

(xvii) Any planned software / hardware downtime would not be included in the calculation of software / hardware availability, in that case;

(a) SI will have to take written approval from the DIT(S) at-least 5 days in advance.

(b) Any planned outage should not be more than 60 minutes and that too the planned outage should be done during the non- office hours (8 PM to 8 AM).

(c) All SLA will be calculated on per-site basis.

4. SCOPE OF WORK

This RFP is meant to invite proposals from interested bidders (selected bidder is referred to as System Integrator (SI) in this document) for Supply, Installation, Commissioning, Operating & Maintenance of CCTV Surveillance, Access Control & Security Scanning System at Aayakar Bhawan, Vaishali, Ghaziabad. SI needs to provide a customized solution to DIT(S) which includes but not limited to hardware, software, networking, cabling etc. The scope of work comprises of the following aspects:

- CCTV surveillance
- Access control
- Security scanning
- Networking and infrastructure
- Manpower
- Physical security compliance

4.1 CCTV Surveillance

The SI would be responsible for the supply, installation, commissioning and maintenance of CCTV Surveillance system.

i. CCTV system shall be provided for obtaining live view of the authorized / unauthorized entry, unauthorized intrusion, abnormal conditions in process areas and recording the events for future investigation.

ii. The CCTV system shall be integrated for escalation of violations in security protocols and unauthorized intrusion into the facility. The integration shall be carried out at higher level without use of dry contact/physical wired connections between the systems.

iii. The high level interfaces shall facilitate higher number of alarms being passed between the systems using data interface. The data interfaces shall be based on industry standard open standard protocols.

iv. The CCTV surveillance system shall be used to monitor the perimeter for unauthorized entry in to the premises and associated facilities by breaching the perimeter of the building and common areas.

v. The CCTV System shall be an integrated system for the building with IP based camera and centralized server with storage.

vi. All recorded data whether in digital/analogue format or as hard copy shall be handled in strict confidence with reasonable physical and logical controls.

vii. Access to CCTV monitoring screen shall be restricted

viii. CCTV surveillance system shall comprise ofCameras, Video Monitoring System, Storage and Networking.

4.1.1 Cameras

The SI would be responsible for the supply, installation, commissioning and maintenance of three types of cameras i.e. The Infra-Red Pan Tilt Zoom Camera (IR-PTZ), Bullet Camera and Dome Camera.

i. The Infra-Red Pan Tilt Zoom Camera (IR-PTZ) cameras shall be installed at the entry gates to monitor personnel and vehicles entering the premises i.e. Aayakar Bhawan, Vaishali. This is in order to clearly identify personnel and vehicle numbers, vehicle types in case of incident investigation. Two cameras shall be positioned at different heights to view inside of Cars driver’s cabin.

ii. Bullet Camera shall be placed on the outside premises to monitor the common area like annexe, walls etc.

iii. Building indoors shall be provided with DOME cameras to monitor the common areas like lobby, staircase, corridor, lift lobby etc.

iv. The number of cameras and their indicative technical specifications are given in Annexure B and Annexure C respectively.

v. Maximum coverage shall be achieved by positioning the cameras in optimised locations.

vi. Position of cameras shall be closely coordinated with the operations team and security team during the execution stage of the project.

vii. All outdoor cameras shall be installed on wall using with mounting bracket.

viii. Perimeter Security cameras shall be mounted on the boundary wall.

ix. Control Room Operator shall be able to view video from multiple cameras on a single screen or multiple screens in the Monitoring Centre.

x. CCTV Surveillance System shall send two streams of video into the network. One of the streams shall be used for live view and the second stream is sent to the network video recorder for storage.

xi. It shall be possible to configure at least three zones on the area being viewed by the camera. The size of the zones shall be configurable.

xii. The system shall also provide facility to initiate an alarm using motion detection in any single zone or a combination of any two or three zones.

4.1.2 Video Monitoring System(with Software)

The SI would be responsible for the supply, installation, commissioning and maintenance of video management server and storage unit.

i. CCTV central equipment shall be installed at the Monitoring Room.

ii. SI shall provide and install the servers and other equipments in Racks.

iii. Central Monitoring Centre shall be provided with 42" High definition LED monitor and client workstation for viewing of video.

iv. An additional 42" High definition LED monitor and client workstation will be provided at a mutually agreed place.

v. The number of devices/equipment and their indicative technical specifications are given in Annexure B and Annexure C respectively.

4.1.3 Storage

Network Video Storage unit shall be sized to retain 30 days of video from all the cameras in accordance with MHA O.M. No. D-32018/3/2015/SSO(Pt.) dated 20.04.2015.Data pertaining to any security incidents which warrant investigation shall be retained for a minimum period of 1 year or till closure of case whichever is later or as required.

4.2 Access control

The SI would be responsible for the supply, installation, commissioning, operating and maintenance of a comprehensive access control system in Aayakar Bhawan, Vaishali building, premises of DIT(S).

i. Only contactless smart card should be used having reader at both sides so that the same may be used for both entry and exit.

ii. Visitors to be issued with access cards which will help them to gain entry inside the building at the ground floor lift lobby.

iii. The system should have the ability to block the card of departmental personnel / vendors' employee's registration in case of their transfer / retirement/termination from the service or any other condition.

iv. The number of devices/equipments and their indicative technical specifications are given in Annexure B and Annexure C respectively.

4.2.1 Access card reader

The card readers should be mountable on standard gang boxes.

i. The Read Range of the Card Reader should be at least 10 cm.

ii. A visual display LED should be provided on the Reader surface. It should preferably be Red when powered on and ready to read a card. When a Card is presented, it should turn Green and remain so for a period of a minimum 1 second (programmable).

iii. A Beep Tone should be generated to indicate acceptance of the card. Door remaining open beyond 5 sec should give an alarm.

iv. The Card Reader should be suitable for outdoor use as well as indoor use.

4.2.2 Access Controller

The Access Control system shall be used to serve the objective of allowing entry and exit to authorised personnel only.

i. Contactless card readers integrated shall be used for entry/exit control.

ii. When Power is on, the Reader should conduct a self-diagnostic test and it should be possible to test the card reader from the PC connected to the Door Controllers.

iii. It should have a Real Time Clock, which should be synchronized with the Central Controller. All transactions shall have an auto date-time stamp generated by the card reader

4.2.3 Flap Barrier

The SI would be responsible for the supply, installation, commissioning and maintenance ofContactless smart card reading device along with the Flap barriers for both ingress as well as egress.

i. The system should have the ability to generate report of entry and exit of each person.

ii. The access control data should be available only to the authorized personnel and it should be encrypted and un-editable.

iii. DIT(S) currently has an estimated 150 departmental personnel and 600outsourced employees working in the building.

iv. The system should be programmable for multiple entries, the records of all of which should be available for every individual (staff/outsourced employee/visitor) for a period of 30 days, beyond which the records could be overwritten. Data should be archived, backed up and retrieved, whenever it is required. However, for the staff and outsourced employees, the first entry and the last exit for the day should be taken into account for registering the attendance.

v. Card issuance process should have an authorization system that will prevent a card being issued / printed until authorizations have been completed.

vi. Temporary access system should be available after proper authorization.

vii. Overriding features should be available to take care of unexpected circumstances such as auto release of door lock opening in case of an emergency.

viii. Further a manual switch/lever be provided to deactivate all Flap Barriers in case of any emergency in the building.

4.2.4 Access Control Cabling

SI will be required to undertake all the necessary wiring required to make the project smooth and seamless.

4.2.5 Visitor Management System

The SI would be responsible for the supply, installation, commissioning and maintenance of Visitor Management System

i. The system should have the facility to record photograph, Mobile number and copy of ID.
ii. Speed check-in for frequent visitors should be in place.
iii. Self Service kiosks to enable visitors to register themselves without having to wait for the receptionist.
iv. Ability for pre-registration of guests based on the approval of DIT(S)
v. During overstay, notification may be sent to the visitor
vi. Customised visitor pass should be provided.
vii. Should provide detailed MIS, query reports etc.

4.2.6 Access Card

The contactless multi-application card shall incorporate radio frequency identification electronics into a thin durable polycarbonate package of not more than 2-3 mm. ISO size cards (Standard Credit Card size) can be offered as an option.

i. The card shall be thin and flexible enough to be carried in a wallet. It shall have extremely consistent read range that is not affected by body shielding, environmental conditions and when close to metal objects.
ii. The card-encoding format shall be so designed that additional cards can be ordered at a subsequent date without upgrading firmware in the existing readers. The card shall offer passive and no battery designed, allowing an infinite number of reads

4.2.7 Boom Barrier

The SI would be responsible for the supply, installation, commissioning and maintenance of boom barrier gate system at the entrance and exit of Aayakar Bhawan, Vaishali.

i. Barrier should remain in open position for optimal period of time for the vehicle to pass at entrance and exit.

ii. Provision to capture image of vehicle including registration plate number of every vehicle entering and leaving Aayakar Bhawan, Vaishali premises and all the information related to the same should be stored at a central server.

iii. Upon horizontal impact by a vehicle, the barrier arm alarm shall be automatically raised and sent to the server and monitoring console.

iv. An alert should be sent to the console and server to ensure that the administrator is informed, that the barrier is not attached or barrier breakage has occurred.

v. All vehicular passages during the period that the barrier is not attached, should be recorded and displayed in the reports separately

4.3 Security Scanning

The SI would be responsible for the supply, installation, commissioning and maintenance of X-ray baggage scanner, door frame metal detector and hand held metal detector.

i. The SI shall be responsible for the statutory approval for operating the procured equipment.

ii. SI has to submit all the necessary certificates for the furnishing products and services to DIT(S) for facilitating the statutory submission and approval process.

iii. The number of devices/equipment and their indicative technical specifications are given in Annexure B and Annexure C respectively.

4.3.1 X-ray Baggage Scanner

X-ray screening equipment is required for use in detecting both metallic and non-metallic objects.

i. The list of items to be identified includes: firearms (both metallic and non-metallic), firearms components, ammunition (all calibres), grenades and other fragmentation/blast weapons, knives, batons, swords, explosives, detonators and timing devices, electrical and electronic items, power sources etc.

ii. The steel roller beds and platforms, tunnel I/O housing, sideguards must facilitate placing of baggage at the input and output points.

iii. The keyboard and TV monitor can be operated remotely.

iv. The x-ray machine must have the readiness of networking. The system can be integrated into network solutions.

4.3.2 Door Frame Metal Detector

The metal detector shall consist of a free standing walk-through frame with an integral control unit, and shall be suitable to detect metallic objects on a person by means of the magnetic field principle.

i. The metal detector shall be suitable to detect ferrous and non-ferrous metals.

ii. The metal detector shall be equipped to eliminate false alarms.

iii. The metal detector shall scan the entire walk through area and detect metal objects on a person passing through to the levels as specified.

iv. The metal detector shall incorporate self-test button to confirm that the system is operating correctly.

v. The programme and sensitivity push buttons shall be so arranged that tampering by unauthorized persons is entirely eliminated.

vi. The metal detector shall not be adversely affected by stationary metal bars or structures in the vicinity of the unit or moving metal near the archway.

vii. It should be possible to use equipment such as personal radios, portable telephones and x-ray monitors without causing spurious alarms. The metal detector shall be capable of operating adjacent to and X-Ray inspection unit.

viii. The detector is intended for indoor use.

4.3.3 Hand Held Metal Detector

The Hand Held Metal Detector must have battery life of at least 40 hours.

i. The detector shall provide a visual or audible indicator to alert the operator of the battery condition.

ii. The detection performance specifications shall be tested using the detection sensitivity setting that is specified in specification.

iii. The detector shall have a power on/off switch.

iv. The detector shall have a means for selectively disabling the audible alarm.

4.4 Networking and Infrastructure

The SI would be responsible for the supply, installation, commissioning and maintenance of all networking equipment related to the scope of work.

i. CCTV IP cameras shall be connected via CAT6 cables / Optical Fibre Cable (OFC) to the Ethernet Switch (Layer2 and Layer3).

ii. A separate local area network with dedicated Ethernet switches shall be implemented to create a new domain for CCTV, Access Control System and Security Scanning System.

iii. The IP Based Video Management System shall provide an open standard interface for high level integration with Access Control system for moving cameras to preset positions in case of an alarm or an event.

iv. SI should also provide Network Monitoring System (NMS) for network monitoring on a network PC.

v. The number of devices/equipment and their indicative technical specifications are given in Annexure B and Annexure C respectively.

Note: In addition to above, SI shall also provide all the necessary hardware/software/accessories including related groundwork for complete installation and functioning of the security equipments to be installed.

4.5 Manpower

SI shall deploy an on-site team including Security System Manager to look after the entire operations of the project, and further coordination with the team. The SI would be responsible for managing operations on a day-to-day basis. The SI is required to provide appropriate number of manpower to perform the activities. The minimum manpower resources to be provisioned by the SI (along with their responsibilities) are as under:

Position	Resources	Responsibilities
Security System Manager	1	• Managing and leading the project team. • Managing co-ordination of the partners and working groups engaged in project work. • Developing and maintaining a detailed project plan. • Managing project deliverables in line with the project plan. • Recording and managing project issues and escalating where necessary. • Resolving cross-functional issues • Monitoring project progress and performance. • To maintain liaison with the Police and other Authorities regarding investigation of any untoward incident under prior information to DIT(S) • Should be available during Business Hours on all working days and as per exigencies of work requirement.

Position	Resources	Responsibilities
Technical Support Engineer	1	• Operation and maintenance of equipment/device and integration • Monitor network performance and integrity • Create, oversee and test security measures. • Maintain complete technical documentation • Suggest improvements to performance, capacity and scalability • Should be available during Business Hours on all working days and as per exigencies of work requirement.
Control Room Operator	3	• Maintaining the control centre equipment. • Verify that all external cameras are set up and broadcasting, and that all the video storage facilities are online and functioning. • Ensure that network drive capture systems have enough free space available for the next 24 hours. • Should keep a written log of any suspicious activities captured by the surveillance equipment. • One person in every shift throughout the currency of the contract.

Position	Resources	Responsibilities
X-ray Baggage Scanner Operator	3	• Ensure baggage is placed properly on the feed belt for the X-ray equipment to ensure effective image production • Prevent unsuitable items from being placed on the conveyor belt. • Perform correct start-up test procedures for the X-ray equipment at screening point start-up times. • Interpret the X-ray images produced by the X-ray equipment. • Selects bags that might contain a prohibited article (or any item that cannot be positively identified) for further processing by hand search and application of trace technology. • One personin every shift throughout the currency of the contract.

4.6 Qualification & Experience Requirement

Position	**Qualification & Experience**
Security System Manager	• BE / MCA • 5 years of experience in related work • Preferably having previous experience in corporate security management.
Technical Support Engineer	• BE / MCA • 3 years of experience implementation of projects of CCTV, access control; Network etc.
Control Room Operator	• Any Graduate • 2 years of experience in Monitoring Centre
X-ray Baggage Scanner Operator	• 12th Pass • 1 year of experience in Operating Baggage Scanner

4.7 Physical Security Compliance

The Information Security Guidelines related to physical and environmental security is given at Annexure A. At present, CPWD handles the fire-fighting equipment, electrical works, smoke detectors, sprinklers etc. Security guards are provided by the integrated facility management services.

The SI would be responsible for conducting surveillance audits on quarterly basis. The focus of surveillance audits will be to ensure continued compliance with the security policies and guidelines.

This area of work will cover the following:

i. Whether the entire system is functioning in line with the relevant security guidelines.

ii. Whether the relevant security controls are effective.

iii. Whether the standard operating procedures (SOP) are followed.

iv. Submit report listing the non-compliance with recommendations.

5. Annexure A: Physical Security Guidelines

5.1 Background

5.1.1. Physical aspects have a role in determining how information and information systems are housed in a facility, who can possibly reach physical systems, which way one can enter or exit from the facility, what can human elements physically do with the system housed in a facility and what will be impact of regional physical events on the particular facilities

5.1.2. Physical security in an important component of information security and requires a careful attention in planning, selecting countermeasures, deploying controls, ensuring secure operations and respond in case of an event

5.1.3. Physical security is not only restricted to barriers or locks but have evolved with the use of access control measures, risk based or multifactor authentications, monitoring cameras, alarms, intrusion detectors, etc.

5.2 Relevance of domain to information security

5.2.1. Lack of due consideration to the area and to the choice of the building may expose information and IT systems to threats. Choice of the area, building architecture and plan have a significant impact on security posture of information and information systems

5.2.2. Insufficient entry controls may give access to unintended persons. It may allow entry of unauthorized assets or easy passage of sensitive assets from premises

5.2.3. Without adequate interior physical control, unauthorized personnel may gain access to sensitive areas. Instances such as theft of information may remain undetected

5.2.4. Without processes for physical access provisioning and deprovisioning, governing access to the sensitive physical locations will remain a challenging task. This will have serious impact on security of information and information during their life cycle in a particular physical facility

5.3 Physical and environmental security guidelines

5.3.1. **Map and characteristics of physical facilities:** The organization must create an map of access point and information assets and systems housed within **PH.G1**

5.3.2. **Protection from hazard:** The organization must ensure that all facilities housing information systems and assets are provided **PH.G2** with adequate physical security measures, which include protection from natural and man-made hazard

Physical boundary protection: The organization must deploy an adequate level of perimeter security measures such as barriers, fencing, protective lighting, etc. **PH.G3**

5.3.3. **Restricting entry:** The organization must deploy an adequate level of countermeasures for restricting the entry to the facilities only to authorized persons **PH.G4**

5.3.4. **Interior security:** The organization must ensure that all information systems and assets are accessed by only authorized staff and protected by adequate interior security measures **PH.G5**

5.3.5. **Security zones:** The organization must ensure that appropriate zones are created to separate areas accessed by visitors from areas housing classified information assets and systems **PH.G6**

a. **Basis information classification:** Appropriate security zones must be created inside the premises/ building based on the location of information assets and systems, commensurate with the classification of information

b. **Marking of zones:** Zones must be clearly marked to indicate type of personnel allowed access to the said zone within the premise

c. **Security and monitoring of zones:** Strict security measures in addition to round the clock monitoring of such areas must be done

5.3.6. **Access to restricted area:** Access of people and equipment movement and disposal from the restricted area should be regulated and governed. A special care must be taken for wearable devices. Such clearances should be done by the concerned head of the department. The organization must establish a methodology to ensure coordination between internal functions and staff for the same **PH.G7**

5.3.7. **Physical activity monitoring and review:** All physical access to information assets and systems should be monitored and tracked. User should not be allowed to carry external devices such as laptops; USB drives etc. without prior approval and authorization, into areas which house critical information infrastructure such as data centers etc. **PH.G8**

5.4. Physical and environmental security controls

5.4.1. **Map and characteristics of physical facilities:** The organization must obtain visibility over physical facilities and information **PH.C1** systems housed within

a. A list of persons who are authorized to gain access to information assets and systems housed in data centers or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and should be reviewed periodically

5.4.2. **Hazard assessment:** The facility housing information assets and systems must be protected from natural hazard and man-made hazard. All facilities located in geographically vulnerable areas must undergo annual assessment to check structural strength **PH.C2**

5.4.3. **Hazard protection:** All facilities must be equipped with adequate equipment to counter man-made disasters or accidents such as fire. The facility should have a combination of hazard detection and control measures such as smoke sensors, sprinklers, fire extinguishers etc. Other sensors and alarms should also be installed for early warning **PH.C3**

5.4.4. **Securing gateways:** All entry and exit points to facilities housing information assets and systems must be secured by deploying manpower and appropriate technological solutions **PH.C4**

5.4.5. **Identity badges:** The entry to a facility is restricted to only those users who provide proof of their organizational identity. Users must be aware of the importance of carrying their identity proof with them **PH.C5**

5.4.6. **Entry of visitors & external service providers:** the organization must defineprocess for allowing and revoking access to visitors, partners, third-party service providers and support services **PH.C6**

5.4.7. **Visitor verification:** All visitors to the facility must only be permitted to enter post validation from concerned employee. Visitor must be instructed to record their identity credentials into the visitor register prior to permitting them inside the facility **PH.C7**

5.4.8. **Infrastructure protection:** Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage **PH.C8**

5.4.9. **Guarding facility:** The organization must ensure that an adequate number of security guards are deployed at the facilities **PH.C9**

5.4.10. **Vehicle entry:** Ensure that an adequate level of security measures are implemented for vehicle entry & exit, vehicle parking **PH.C10** areas, loading/unloading docks, storage areas, manholes, and any other area that may provide passage for physical intrusion

5.4.11. **Correlation between physical and logical security:** The instances of physical access should be analyzed with logical access instances. Restrictions should be imposed for on premise access of information systems to unauthorized personnel. **PH.C11**

5.4.12. **Monitoring & surveillance:** All entry and exit points should be under surveillance round the clock to look for suspicious activity. Further, all security zones inside the facility/ building must be secured by deploying manpower and appropriate security technologies **PH.C12**

5.4.13. **Disposal of equipment:** Physical disposal of computer or electronic office equipment containing non-volatile data storage capabilities must be checked and examined to ensure all information has been removed. Destruction, overwriting or reformatting of media must be approved and performed with appropriate facilities or techniques such as degaussing of hard drives, secure delete technologies etc. **PH.C13**

5.4.14. **Protection of information assets and systems:** All information assets and systems must be protected with appropriate access control methodologies such as authorized log-in and password control, smart cards or biometric access **PH.C14**

5.4.15. **Authorization for change:** Ensure that security authorization is performed for all changes pertaining to physical security, instances that may introduce security vulnerabilities and exception to the policy **PH.C15**

5.4.16. **Inactivity timeout:** All information systems must be configured to time-out a user’s activity post inactivity for a designated period of time **PH.C16**

5.4.17. **Protection of access keys and methodology:** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures **PH.C17**

5.4.18. **Shoulder surfing:** The display screen of an information system on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it **PH.C18**

5.4.19. **Categorization of zones:** The facilities in the organization must be categorized based on parameters such as the sensitivity of information in the facility, roles of employees in facilities, operational nature of facility, influx of visitors etc. **PH.C19**

5.4.20. **Access to restricted areas:** Visitors requiring access to restricted areas, in –order to perform maintenance tasks or activities must be accompanied by authorized personnel from the concerned department at all times. A record of all equipment being carried inside the facility must be maintained along with equipment identification details. Similarly a record of all equipment being carried outside the facility must be recorded and allowed post validation and written consent from employee concerned **PH.C20**

5.4.21. **Visitor device management:** Visitors must be instructed to avoid carrying any personal computing devices or storage devices inside facilities housing classified information, unless written permission is obtained from the head of the department **PH.C21**

5.4.22. **Physical access auditing and review:** All attempts of physical access must be audited on a periodic basis **PH.C22**

5.5. Physical security implementation guidelines

5.5.1. **Map and characteristics of physical facilities:** The organization must appropriately position security and monitoring measures commensurate with criticality of Physical facilities, information and IT systems housed within these facilities **PH.IG1**

a. Create map of facilities, their entry & exit points, deployment of IT systems and people

b. Create list of authorized personnel, permitted to access areas/ facility housing sensitive information systems/ devices, should be maintained at all entry points

c. Physical access to such areas/facility must be granted only post verification of person as well as by user authentication by use of smart cards, etc.

5.5.2. **Hazard assessment:** The organization must undergo hazard assessment at regular intervals to counter disasters or accidents such as fire safety risk assessment, seismic safety assessment, flood control assessment and other natural calamities amongst others **PH.IG2**

5.5.3. **Hazard protection:** The organization must deploy sufficient tools, techniques, equipment etc., to deal with hazard. Capability for detection, prevention and control measures such as fire alarms, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings must be available in each facility housing classified information **PH.IG3**

5.5.4. **Securing gateways:** All entry and exit points to facilities/areas housing classified information in an organization must have biometric access controls such as fingerprint scanners or other similar gateway access control mechanisms **PH.IG4**

5.5.5. **Identity badges:** Theorganization must issue photo identity cards with additional security features such as smart chips to employees for identification and entry to facilities **PH.IG5**

a. Appropriate measures must be undertaken to prevent tailgating inside the organizations facility

5.5.6. **Entry of visitors & external service providers:** The organization should maintain records for visitor entry such as name of visitor, time of visit, concerned person for visit, purpose of visit, address of the visitor, phone number of the visitor, ID proof presented, devices on-person etc. **PH.IG6**

b. Entry by visitors such as vendor support staff, maintenance staff, project teams or other external parties, must not be allowed unless accompanied by authorized staff

c. Authorized personnel permitted to enter the data center or computer room must display their identification cards at all instances

d. Visitor access record shall be kept and properly maintained for audit purpose. The access records may include details such as name and organisation of the person visiting, signature of the visitor, date of access, time of entry and departure, purpose of visit, etc.

e. The passage between the data centre/computer room and the data control office, if any, should not be publicly accessible in order to avoid the taking away of material from the data centre/computer room without being noticed

5.5.7. **Visitor verification:** Visitor entry must be permitted only if prior notification has been shared via email from the concerned personnel. **PH.IG7**

a. Visitors must present a valid photo identification card, preferably issued by the Government of India at the reception, for verification

b. Visitors must always be escorted by the concerned person into the designated meeting area in the facility

c. Visitors should be issued a temporary identity card that identifies them as a visitor and must be returned to issuing authority while leaving the premises after marking out time in the visitor’s record

5.5.8. **Infrastructure protection:** **PH.IG8**

a. Power and telecommunication lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection

b. Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas

c. Power cables and switching centers should be segregated from communication cables to prevent interference

5.5.9. **Guarding facility:** Background checks of all private guards manning the facility should be conducted prior to employment/ deployment. Details such as address verification, criminal records, past experience, references, family details, medical records must be maintained as a minimum **PH.IG9**

a. Ensure that background checks and credibility is established prior to recruitment of guards. In- case guards are hired from a third party organization a stringent process to verify and establish credibility of the third-party organization must also be undertaken

b. The organization must conduct regular trainings for security guards to handle routine security operations as well as security incidents, physical intrusions, awareness about new storage devices, etc.

5.5.10. **Vehicle entry:** Adequate security measures should be adopted at vehicle entry, exit and parking areas such as deploying physical barriers, manual inspection of vehicles, security lighting, video surveillance, deploying adequate security guards etc. **PH.IG10**

5.5.11. **Correlation between physical and logical security:** Physical security and logical security linkages must be created **PH.IG11**

a. Only approved personnel should have physical access to facility housing systems or devices which enable physical or logical access to sensitive data and systems. This includes areas within the facility which house backup tapes, servers, cables and communication systems etc.

b. Access controls should encompass areas containing system hardware, network wiring, backup media, and any other elements required for the system's operation

5.5.12. **Monitoring & surveillance:** The organization must establish mechanism for 24/7 surveillance of all areas inside the physical perimeter by use of technology such as security cameras (or closed-circuit TV) **PH.IG12**

a. The organization must monitor the areas such as hosting critical/sensitive systems and have video images recorded. The recording of the camera should be retained for at least a month for future review

b. Intruder detection systems can be considered to be installed for areas hosting critical/sensitive systems

5.5.13. **Disposal of equipment:** Destruction and disposal of hard drives/ memory devices should be performed by techniques such as removing magnets, hammering, burning, degaussing, shredding, secure deletion etc. **PH.IG13**

a. Any equipment, being carried out of the facility for disposal, must be authorized by the head of the department, under whom the equipment was deployed as well as the concerned representative of the information security team

5.5.14. **Protection of information assets and systems:** Physical access to information assets and systems must be governed by employing techniques such as biometric access, smart cards, passwords etc. **PH.IG14**

5.5.15. **Authorization for change:** Any modification or changes to the physical security layout/ established procedure must be done post documented approval of concerned authority in the security team/ Head of the department **PH.IG15**

5.5.16. **Inactivity timeout:** All information systems should be configured to automatically lock the computer system after 10 minutes of inactivity **PH.IG16**

5.5.17. **Protection of access keys: :** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures **PH.IG17**

a. Maintain a record of all physical access keys by capturing details such as serial number, card ID

b. Create a mapping of physical cards issued with details of person authorized to use the same

c. Establish governance and audit procedures to manage issue of all physical access cards and eventual return to concerned authority on employee departure or revocation of access rights of individual authorized to access using physical cards

5.5.18. **Shoulder surfing:** Information systems containing classified information should be secured, to avoid shoulder surfing, by deploying privacy filter, positioning the systems to reduce chances of unauthorized viewing **PH.IG18**

5.5.19. **Categorization of zones:** The facility should be categorized as follows: **PH.IG19**

a. **Public zone:** where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings

b. **Reception zone**: where the transition from a public zone to a restricted-access area is demarcated and controlled. It is typically located at the entry to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons

c. **Operations zone:** an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Examples: typical open office space, or typical electrical room

d. **Security zone:** area to which access is limited to authorized personnel, and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Example: an area where secret information is processed or stored

e. **High security zone**: an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications, monitored continuously and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel

5.5.20. **Access to restricted areas:** Visitors requiring access to restricted areas must be accompanied by authorized personnel. Visitor details such as name of the visitor, time of visit, purpose of visit, serial number of the equipment (if being carried), name of authorized person, signature of authorized person etc. must be maintained by the security personnel responsible for the area/facility **PH.IG20**

a. In case, any equipment is being carried out by the visitor, appropriate written authorization granted by the head of the department/ concerned official must be presented to security personnel

b. An inventory of all equipment taken out of the facility should be maintained. Details such as equipment name, serial number, model number, department/ owner, name of approver etc. must be maintained

c. The information security team must co-authorize the removal of equipment from its deployment site

5.5.21. **Visitor device management:** Visitors must not be allowed to carry personal computing or storage devices such as USB, laptop, hard drive, CD/DVD etc. unless written permission is obtained from head of department. **PH.IG21**

a. Wearable devices: Visitors must be prohibited from carrying any wearable computing and processing devices such as smart watch's, glass or similar equipment

b. All visitors and Third parties authorized to carry information processing equipment (like Laptops, Ultra books, PDAs) or Media (like Mobile phones with cameras, DVD/CDs, Tapes, Removable storage), shall be asked to declare such assets. They will be issued a returnable gate pass containing the date, time of entry and departure along the type of equipment and its serial number, if applicable. The same shall also be recorded in a register at the security gate.

c. Equipment like laptops, hard disks, tape drives, camera mobile phones, etc. shall not be allowed inside the restricted areas, shared services area, etc. unless authorized by the concerned authority

5.5.22. **Physical access auditing and review:** All attempts of physical access must be captured in logs and audited for illegal access attempts, number of access attempts, period of access, facilities visited etc. The following steps should be undertaken **PH.IG22**

1. a. Enabling and collecting logs physical devices
2. b. Writing rules to correlate logs to identify physical security incidents
3. c. Integrating physical security logs with logical security logs
4. d. Integrating physical security with SIEM solutions
5. e. Real time monitoring of physical security logs for classified information

5.6. Adoption matrix for Physical Security

	Top secret	**Secret**	**Confidential**	**Restricted**	**Unclassified**
Guidelines					
Map and characteristics of physical facilities	PH.G1	PH.G1	PH.G1	PH.G1	
Protection from hazard	PH.G2	PH.G2	PH.G2	PH.G2	PH.G2
Physical boundary protection	PH.G3	PH.G3	PH.G3	PH.G3	PH.G3
Restricting entry	PH.G4	PH.G4	PH.G4		
Interior security	PH.G5	PH.G5	PH.G5	PH.G5	
Security zones	PH.G6	PH.G6	PH.G6	PH.G6	
Access to restricted area	PH.G7	PH.G7	PH.G7	PH.G7	
Physical activity monitoring and review	PH.G8	PH.G8	PH.G8	PH.G8	
Controls					
Map and characteristics of physical facilities	PH.C1	PH.C1	PH.C1	PH.C1	
Hazard assessment	PH.C2	PH.C2	PH.C2	PH.C2	PH.C2
Hazard protection	PH.C3	PH.C3	PH.C3	PH.C3	PH.C3
Securing gateways	PH.C4	PH.C4	PH.C4	PH.C4	
Identity badges	PH.C5	PH.C5	PH.C5	PH.C5	
Entry of visitors & external service providers	PH.C6	PH.C6	PH.C6	PH.C6	
Visitor verification	PH.C7	PH.C7	PH.C7	PH.C1	
Infrastructure protection	PH.C8	PH.C8	PH.C8	PH.C2	PH.C8
Guarding facility	PH.C9	PH.C9	PH.C9	PH.C9	
Vehicle entry	PH.C10	PH.C10	PH.C10	PH.C10	

	Top secret	Secret	Confidential	Restricted	Unclassified
Correlation between physical and logical security	PH.C11	PH.C11	PH.C11		
Monitoring & surveillance	PH.C12	PH.C12	PH.C12		
Disposal of equipment	PH.C13	PH.C13	PH.C13	PH.C13	
Protection of information assets and systems	PH.C14	PH.C14	PH.C14		
Authorization for change	PH.C15	PH.C15	PH.C15		
Inactivity timeout	PH.C16	PH.C16	PH.C16	PH.C16	
Protection of access keys and methodology	PH.C17	PH.C17	PH.C17	PH.C17	
Shoulder surfing	PH.C18	PH.C18	PH.C18	PH.C18	
Categorization of zones	PH.C19	PH.C19	PH.C19	PH.C19	
Access to restricted areas	PH.C20	PH.C20	PH.C20	PH.C20	
Visitor device management	PH.C21	PH.C21	PH.C21	PH.C21	
Physical access auditing and review	PH.C22	PH.C22	PH.C22	PH.C22	
Implementation Guidelines					
Map and characteristics of physical facilities	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a) , (b),(c)	
Hazard assessment	PH.IG2	PH.IG2	PH.IG2	PH.IG2	PH.IG2
Hazard protection	PH.IG3	PH.IG3	PH.IG3	PH.IG3	PH.IG3
Securing gateways	PH.IG4	PH.IG4	PH.IG4	PH.IG4	
Identity badges	PH.IG5, PH.IG5(a)	PH.IG5, PH.IG5(a)	PH.IG5, PH.IG5(a)	PH.IG5	

	Top secret	Secret	Confidential	Restricted	Unclassified
Entry of visitors & external service providers	PH.IG6, PH.IG6 (a) to (e)	PH.IG6, PH.IG6 (a) to (e)	PH.IG6, PH.IG6 (a) to (e)	PH.IG6	
Visitor verification	PH.IG7, PH.IG7(a),(b),(c)	PH.IG7, PH.IG7(a),(b) , (c)	PH.IG7, PH.IG7(a),(b),(c)	PH.IG7, PH.IG7 (a),(b) ,(c)	
Infrastructure protection	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)
Guarding facility	PH.IG9, PH.IG9(a),(b)	PH.IG9, PH.IG9 (a),(b)	PH.IG9, PH.IG9(a)	PH.IG9	
Vehicle entry	PH.IG10	PH.IG10	PH.IG10		
Correlation between physical and logical security	PH.IG11, PH.IG11(a),(b)	PH.IG11, PH.IG11(a),(b)	PH.IG11, PH.IG11(a),(b)		
Monitoring & surveillance	PH.IG12, PH.IG12(a),(b)	PH.IG12, PH.IG12(a),(b)	PH.IG12, PH.IG12(a),(b)		
Disposal of equipment	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	
Protection of information assets and systems	PH.IG14	PH.IG14	PH.IG14		
Authorization for change	PH.IG15	PH.IG15	PH.IG15		
Inactivity timeout	PH.IG16	PH.IG16	PH.IG16	PH.IG16	
Protection of access keys	PH.IG17, PH.IG17 (a),(b),(c)	PH.IG17, PH.IG17 (a),(b),(c)	PH.IG17, PH.IG17(c)		
Shoulder surfing	PH.IG18	PH.IG18	PH.IG18	PH.IG18	

	Top secret	**Secret**	**Confidential**	**Restricted**	**Unclassified**
Categorization of zones	PH.IG19, PH.IG13(e)	PH.IG19, PH.IG13(d)	PH.IG19, PH.IG13(d)	PH.IG19, PH.IG13(c)	
Access to restricted areas	PH.IG20, PH.IG20 (a),(b),(c)	PH.IG20, PH.IG20 (a),(b),(c)	PH.IG20, PH.IG20(a),(b),(c)	PH.IG20	
Visitor device management	PH.IG21, PH.IG21 (a),(b),(c)	PH.IG21, PH.IG21 (a),(b),(c)	PH.IG21, PH.IG21 (a),(b)	PH.IG21, PH.IG21 (a),(b)	
Physical access auditing and review	PH.IG22, PH.IG22 (a),(b),(c)(d)(e)	PH.IG22, PH.IG22 (a),(b),(c)(d)(e)	PH.IG22, PH.IG22 (a),(b)	PH.IG22, PH.IG22 (a),(b)	

6. Annexure B: Bill of Material (Indicative)

S. No	Description of Item	Qty
1.	Infra-Red Pan Tilt Zoom Camera (IR- PTZ)	10
2.	Bullet Camera with built in IR	50
3.	DOME Camera with built in IR	140
4.	Video Monitoring System (with Software)	1
5.	Storage	250 TB
6.	LED Display	6
7.	Server for Network Video Recorder	5
8.	Work Station for Local Viewing	6
9.	Access card reader	24
10.	Access Card	1000
11.	Flap Barrier	3
12.	Access Controller	3
13.	Boom Barrier	2
14.	Visitor Management Software (With Workstation)	1
15.	ID Badge Printer with consumable to print 1000 cards	1
16.	X-ray Baggage Scanner	1
17.	Door Frame Metal Detector	3

S. No	Description of Item	Qty
18.	Handheld Metal Detector	4
19.	Network Monitoring System {NMS}	1
20.	Networking (including Switches)	1
21.	Others (if any)	

7. Annexure C: Technical Specifications (Indicative)

The indicative technical specifications are given as under.

7.1 CCTV Surveillance

7.1.1 Infra-Red Pan Tilt Zoom Camera (IR- PTZ)

Make: Sony/Panasonic/Bosch/Pelco

S. No	Specification	Complied (Yes / No)
1.	Camera Image Sensor : 1/3" Progressive Scan CMOS Sensor or better	
2.	Max Video resolution : 3M (2048x1536) or better	
3.	Scanning Mode : Progressive scan	
4.	Shutter Speed : 1/3 ~ 1/10000 secor higher	
5.	Day/Night : IR Cut Filter	
6.	Minimum Illumination Color : 0.1 lx at F1.6	
7.	Minimum Illumination B/W: 0.01 lx at F1.6 or better	
8.	Zoom : 30x Optical Zoom; 10x Digital Zoom; Autofocus	
9.	Focal Length : 4.5-129 mm or better	
10.	Pan : 360°endless	
11.	Tilt: -15°~ 90° ,	
12.	Pan Manual Speed : 0.1°~ 85°/s	
13.	Tilt Manual Speed : 0.1°~ 50°/s	
14.	Presets : 256 or more	
15.	Preset Pan Speed : 9°~ 270°/s	
16.	Preset Tilt Speed : 7°~ 280°/s	
17.	Auto pan ,	

S. No	Specification	Complied (Yes / No)
18.	Privacy Mask : 16	
19.	Video Compression H.264 ,MJPEG	
20.	Auto iris	
21.	Function : Preset / Auto pan	
22.	Auto Flip	
23.	Day / Night: IR Cut Filter Image : On / Off	
24.	Rotation : Flip	
25.	SD Card Support	
26.	Noise Reduction : 2D, 3D	
27.	IR Distance : 100 meters or better	
28.	Network Interface : RJ-45	
29.	Angle of View : 60° (Wide); 2.4° (Tele)	
30.	Wide Dynamic Range 120 dB or better	
31.	No. of Streams : 3 streams or more	
32.	Supported Resolutions : 3M (2048x1536)/ Full HD 1080P / 720P / D1 / CIF	
33.	Supported Protocol : IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
34.	SD Memory Card Feature : 64 GB or better	
35.	Alarm I/O :Input: 2 • Output: 1	
36.	Image Compression: MJPEG / H.264 (MPEG-4 Part 10/AVC) Baseline / Main Profile / High Profile	

S. No	Specification	Complied (Yes / No)
37.	Configurable Image Parameters : White Balance, Noise Reduction, Brightness, Exposure, Sharpness, Saturation , Hue, Privacy Mask, Day/Night Threshold	
38.	Input/ Monitor Output : Support (1 X BNC)	
39.	Audio : Two-way audio	
40.	Max number of user accounts : 20	
41.	Certifications : CE, UL,FCC	
42.	Power Source and Consumption : Should support 802.3at (PoE+), AC 24V,	
43.	Ambient Operating : -10 °C ~ +55 °C	
44.	Temperature/Humidity : 90 % or less (without condensation)	
45.	Dust and water protection : IP 66	
46.	Onvif : ONVIF Profile S	

7.1.2 Bullet Camera

Make: Sony/Panasonic/Bosch/Pelco

S. No	**Specification**	**Complied (Yes / No)**
1.	Camera Image Sensor : 1/2.8" Progressive Scan CMOS Sensor	
2.	Max Video resolution : 3M (2048x1536) or better	
3.	Scanning Mode : Progressive scan	
4.	Shutter Speed : 1 ~ 1/10000 sec.	
5.	Day/Night : IR Cut Filter	
6.	Minimum Illumination Color : 0.04 lx	
7.	Minimum Illumination B/W: 0.002 lx	
8.	Vari Focal Lens : Motorized, Autofocus 2.8 ~ 12 mm lens with P-iris	
9.	Angle of View : 105° (Wide); 38° (Tele)	
10.	Wide Dynamic Range : 120 dB or better	
11.	IR Distance :40 meters or better	
12.	Video Motion Detection : Yes	
13.	No. of Streams : 4 streams or more with at least 2 x H.264 streams at Full HD (1920 x 1080p) or better simultaneously	
14.	Supported Resolutions : 3M (2048x1536)/ Full HD 1080P / SXGA / 720P / XGA / SVGA / D1 / VGA / CIF	
15.	Optical Zoom : 3x or better	
16.	Supported Protocol : IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
17.	SD Memory Card Feature : 64 GB or better	
18.	Alarm I/O : Input: 2 ,Output: 1	

S. No	Specification	Complied (Yes / No)
19.	Security : HTTPS / IP Filter / IEEE 802.1X	
20.	Image Compression.: MJPEG / H.264 (MPEG-4 Part 10/AVC) Baseline / Main Profile / High Profile	
21.	Network Interface : RJ-45, 10/100Mbps Ethernet	
22.	Configurable Image Parameters : Backlight Compensation, White Balance, Noise Reduction, Brightness, Exposure, Sharpness, Contrast, Saturation Hue, Privacy Mask, Day/Night Threshold	
23.	Input/ Monitor Output : 1.0 V [p-p] / 75 Ω BNC	
24.	Audio : Two-way audio	
25.	Audio Compression : G.711, G.726, AAC, LPCM	
26.	Noise Reduction : 3D Motion Compensated Noise Reduction	
27.	Event Notifications : HTTP / FTP / SMTP	
28.	Embedded Video Analytics : Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal	
29.	RS-485 (external control): Supported	
30.	Max number of user accounts : 20	
31.	Certifications : CE, UL,FCC	
32.	Power Source and Consumption : Should support DC 12V, AC 24V, PoE	
33.	Ambient Operating : -10 °C ~ +55 °C	
34.	Temperature/Humidity : 90 % or less (without condensation)	
35.	Dust and water protection : IP 67	
36.	Onvif : ONVIF Profile S	

7.1.3 DOME Camera

Make: Sony/Panasonic/Bosch/Pelco

S. No	Specification	Complied (Yes / No)
1.	Camera Image Sensor : 1/2.8" Progressive Scan CMOS Sensor	
2.	Max Video resolution: 3M (2048x1536) or better	
3.	Scanning Mode: Progressive scan	
4.	Shutter Speed: 1 ~ 1/10000 sec.	
5.	Day/Night: IR Cut Filter	
6.	Minimum Illumination Color: 0.04 lx	
7.	Minimum Illumination B/W: 0.002 lx	
8.	Vari Focal Lens: Motorized, Autofocus 2.8 ~ 12 mm lens with P-iris	
9.	Angle of View: 105° (Wide); 38° (Tele)	
10.	Wide Dynamic Range: 120 dB or better	
11.	IR Distance : 40 meters or better	
12.	Video Motion Detection : Yes	
13.	No. of Streams : 4 streams or more with at least 2 x H.264 streams at Full HD (1920 x 1080p) or better simultaneously	
14.	Supported Resolutions : 3M (2048x1536)/ Full HD 1080P / SXGA / 720P / XGA / SVGA / D1 / VGA / CIF	
15.	Optical Zoom: 3x or better	
16.	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
17.	SD Memory Card Feature : 64 GB or better	
18.	Alarm I/O : Input: 1 ,Output: 1	

S. No	Specification	Complied (Yes / No)
19.	Security : HTTPS / IP Filter / IEEE 802.1X	
20.	Image Compression: MJPEG / H.264 (MPEG-4 Part 10/AVC) Baseline / Main Profile / High Profile	
21.	Network Interface: RJ-45, 10/100Mbps Ethernet	
22.	Configurable Image Parameters : Backlight Compensation, White Balance, Noise Reduction, Brightness, Exposure, Sharpness, Contrast, Saturation Hue, Privacy Mask, Day/Night Threshold	
23.	Input/ Monitor Output : 1.0 V [p-p] / 75 Ω BNC	
24.	Audio : Two-way audio	
25.	Audio Compression : G.711, G.726, AAC, LPCM	
26.	Noise Reduction : 3D Motion Compensated Noise Reduction	
27.	Event Notifications: HTTP / FTP / SMTP	
28.	Embedded Video Analytics: Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal	
29.	RS-485 (external control) : Supported	
30.	Max number of user accounts : 20	
31.	Impact protection : Vandal proof IK10	
32.	Certifications : CE, UL,FCC	
33.	Power Source and Consumption : Should support DC 12V, AC 24V, PoE	
34.	Ambient Operating : -10 °C ~ +55 °C:	
35.	Temperature/Humidity : 90 % or less (without condensation)	
36.	Dust and water protection: IP 66	
37.	Onvif: ONVIF Profile S	

7.1.4 Video Monitoring System (With software)

Make: Genetec/Milestone/Bosch/Mirasys/Samsung

S. No	Specification	Complied (Yes / No)
1.	Supported Operating Systems: Linux, Microsoft Windows: 7/8, Microsoft Server 2008 R2/2012, Microsoft Windows Embedded 8 Standard. Support for both 32-bit (x86), 64-bit (x64) versions	
2.	ONVIF Support : ONVIF, ONVIF Profile S Supported Cameras	
3.	Video Stream Formats : MJPEG, MPEG-4, H.264	
4.	Audio Support : 2-way support	
5.	Resolution : Limited only by the camera	
6.	Frame Rate : Limited only by the camera	
7.	Maximum Number of cameras on a single compatible server : 80	
8.	Number of servers in the system : Unlimited	
9.	Number of remote workstations : Unlimited	
10.	Interface Language : English and multi-language support	
11.	Archive Materials Storage Format : In the format received from the IP camera	
12.	Archive Size: Should be able to create different archive sizes per any camera or any group of cameras.	
13.	File Playback Speed : From single-frame playback up to 32x speed up or better	
14.	Auto Zoom : Displaying the separate enlarged area with moving objects	
15.	PTZ cameras : Control of PTZ cameras using the client interface: camera rotation, zoom in/out (optical zoom), focus	

S. No	Specification	Complied (Yes / No)
16.	Panoramic camera support: Support of various modes used in panoramic cameras with just a single VMS license.	
17.	SD card archive support : Integration should be possible	
18.	Cameras auto search : The ability to automatically search for cameras that support ONVIF or UPnP detection protocol in a local network	
19.	Server backup Hot backup: in case of server failure, recording is redirected to a backup server	
20.	Integration with 3rd Party Video Analytics Server: Should support and accept notifications from 3rd Party analytics server.	

S. No	Specification	Complied (Yes / No)
21.	User Interface • Timeline based UI which allows one-click based access to past recordings. • Timeline should always accessible. No separate interface for viewing recordings. • Dragging the timeline should synchronize all camera images to the selected point in time. • The timeline can be hidden so that the camera windows can be shown on the whole screen. • Camera window cloning enables the simultaneous viewing of real-time and recorded image. • VMS should support Calendar search and specific time search • The size and layout of camera windows should be able to be freely adjusted • Window layouts should be able to be saved in shortcut buttons with specific labels • Automatic arrangement of camera windows should be possible • Video Wall support and camera window arrangement functionality • Pre-programmable notifications • Creation and naming of bookmarks of video.	

S. No	Specification	Complied (Yes / No)
22.	Camera Window Tools 6. • Full screen Mode: Should be able to the selected camera in full screen mode • Create video clip: Should be able to create a video clip recording of the visible image. Can be selected in another camera window, which will cause the video clip to continue from that window. (editable video clip) • Quick search from this camera: Should only show the recordings for this camera on the timeline. The playback should jump over motion detections in other areas. • Area search: User should be able to draw areas comprising one or more camera image, and the motion detections of this area will be shown on the timeline. The playback will jump over motion detections in other areas. • Clone window: Should copy the camera window. Should allow simultaneous viewing of the present time and recordings from the same camera with the use of the “Detach from the main timeline” function. • Detach from the main timeline: Should open a separate timeline as a window. The other camera windows should follow the main timeline. • Start recording: Should starts a continuous recording of 1 minute (time adjustable) of this camera image on 1-click. • Customized buttons: Can be used to control gates or other external devices with rule-customized buttons. • Screenshot: Saves the visible image as an image file (JPG, PNG or PDF). Resolution can be selected.	

S. No	Specification	Complied (Yes / No)
23.	Remote Use • Compatible with Windows, Linux and OS X client machines • Should use TCP/IP connection that can be encrypted. • Can be connected to multiple network video servers simultaneously. • Recordings from multiple servers can be synchronized. • Real-time image and recording transfer online, either full quality or compressed quality can be selected. • Notification events and alarms are forwarded directly from the server to the user. • Customized buttons enable the management of different functions, such as recording and saving from connected external devices.	
24.	Notifications • Real-time notification window • Notifications include a screenshot and a description of the event contents • Notification colours should be adjustable • Clicking the notification should open an image recording of the event from the connected camera. • Bookmarks should be able to be saved directly from notifications • Rules should be able to be used to set specific conditions for notifications.	

S. No	Specification	Complied (Yes / No)
25.	Multiple Network Video Recorders Synchronization • Should support viewing synchronized real-time and recorded image feed from multiple servers • Should support saving views comprised of camera feed from multiple recorders • Area search for a combination of cameras from different recorders • Notifications and alarms from multiple recorders simultaneously • Saving merged backup copies and video clips	
26.	Bookmarks • Support saving bookmarks in the timeline • Support naming, editing and removing bookmarks • Bookmarks should be saved in the bookmark list and should also be visible on the timeline. • Bookmarks are saved locally. • Bookmarks can be browsed with the arrow keys, previous/next	
27.	Editable Camera Views • Camera windows can be arranged as wanted • Camera window layouts can be saved and named • Frequently used views can be saved as shortcut buttons • Camera views can contain cameras from multiple recorders	

S. No	Specification	Complied (Yes / No)
28.	Alarm Log • Alarm event programming can be triggered by digital I/O, connection status, video signal loss, alarm lines motion detection and more. • Free text can be assigned to alarms. • Cameras can be selected for specific alarm events. • Alarm events can be browsed in the alarm log for a specific time frame. • Recordings in an event log can be viewed by clicking on the event.	
29.	Video Clips • Time frame and selected cameras: Saves a grid comprising of selected cameras into a single file. • Edited video clip: Records a continuous image of the selected camera window. The source of the video material can be changed by changing the active camera window. • Quick search and area search can be used with the video clip tools. • Save as an AVI file with MPEG4 codec.	
30.	Backup Copies • Saving of full-quality backup copies • The start and end points of the backup file can be freely determined. • Quick search and area search can be used to filter unwanted movement. • Backup copies can be viewed using the remote software. • Quick and area searches can be made in the backup file • Video clips and screenshots can be saved from the backup file.	

S. No	Specification	Complied (Yes / No)
31.	Rules • Rules can be used to control recorder functionality and external devices as well as to send information on different events • One or more conditions are set for the rules. • Conditions can include for example: Schedule, I/O-feed, motion detection, alarm lines, connection loss etc. • Rules are set actions to be performed when rule conditions are met. Actions can include: Digital output control, notification event/alarm, selecting a PTZ preset, saving a bookmark, sending an email message etc.	
32.	User Management • Username and password protection. • Selecting functions and software areas. • Camera access based on user permissions. • Remote access selection for users • Camera control selection for users	
33.	Archival Storage Modes • Storage space is shown as a percentage of total available space. • Recording time can be specified to a date. • User Interface should be able to show the date of the oldest recording	

S. No	Specification	Complied (Yes / No)
34.	Software Motion Detection • Smart Motion detection should function with all types of ONVIF conformant cameras regardless of manufacturer. • Sensitivity and noise reduction should be adjustable. • VMS should index the location of motion in the image for the purposes of area searches. • Separate motion detection areas with different sensitivity can be set for an image. • Areas of the image that should not be recorded can be covered via motion detection.	
35.	Map View • Cameras can be placed in map views and opened directly from the map • There can be multiple maps e.g. for different floors. • Maps can include links to other maps. • Maps are placed in separate movable windows, and several windows can be viewed simultaneously • Maps can be zoomed and moved by using your mouse inside the window. • Camera locations can be edited • Map modification can be turned off	

S. No	Specification	Complied (Yes / No)
36.	Virtual Matrix • Command and Control room interface for real-time surveillance • Virtual matrix can include one or more screens and should support Video Walls. • Includes monitor windows and regular camera windows that can be used to record several views • Image source selection for monitor windows can be automated e.g. based on alarms. • Cameras selected for monitor windows can be controlled with one or more joysticks. • Controlled camera can be selected with joystick buttons or mouse. • Notification events are shown instantaneously from e.g. alarm information or motion detection.	

S. No	Specification	Complied (Yes / No)
37.	Diagnostic • Notification events can be set in the system in different ways, such as rules, motion detection from image, external I/O data, or internal software command. • Notifications can contain a free text field, event colours are customisable, and a preview image is attached to the notification. • Status information and preset alarms are saved in the alarm log in chronological order • The alarm log contains an acknowledgement functionality. • User can access a recording attached to a notification by one click • VMS should send notifications of possible system errors, such as camera or server connection errors, recording errors, hard drive faults and power supply faults (fault-tolerant servers). • System should be capable of integrating latest technology related to artificial Intelligence such as tracking of specified persons, articles, suspicious movements, identifying obtrusive baggage etc.	

7.1.5 LED Display

Make: LG /SAMSUNG /SONY

S. No	Specification	Complied (Yes / No)
1.	Screen Size: 55 inch and above	
2.	Aspect Ratio : 16:09	
3.	Native Resolution : 1920 x 1080 (FHD)	
4.	Brightness : 350 nit or Higher	
5.	Orientation: Portrait & Landscape	
6.	Input: HDMI, USB port	
7.	Output: External Speaker Out	
8.	External Control: RJ45, IR Receiver	
9.	Energy Star: Energy Star 6.0	

7.1.6 Server for Video Monitoring System

Make: Dell/ IBM/ HP

S. No	Specification	Complied (Yes / No)
1.	Min Number of IP Cameras Supported : 70 Channels	
2.	Max Viewing & Recording Resolution : 3MP at 25 FPS or better;	
3.	Processor : Dual Processor: 2 x Intel Xeon E5-2620 v4 2.1GHz or better	
4.	RAM: 16GB or better	
5.	Storage HDD: 8 x SATA HDD Slots with total max storage capacity of 64TB;	
6.	Should be Rack-Mount	
7.	Operating System : Embedded Linux / Windows 2012 R2 Server	
8.	Network: Quad Gigabit Ethernet Interfaces	
9.	Hardware Raid Controller to support Raid 0,1,5,6 or more	
10.	Preinstalled VMS. Licenses required to activate Camera Channels	
11.	Should have Dual Redundant power supply	
12.	Should have Required DVD+/-RW Drive	

7.1.7 Work Station for Local Viewing

Make: Dell/ IBM/ HP

S. No	Specification	Complied (Yes / No)
1.	Operating system : Operating System: Microsoft Windows 7 (32 & 64 bit), 10 (32 & 64 bit), Linux, OS X Yosemite, El Capitan	
2.	Processor : Intel Core i7 or higher	
3.	RAM : 8 GB or more	
4.	Display driver : Intel or Nvidia, 512 MB RAM or more	
5.	Disk space : 1 TB	
6.	Should have DVD+/-RW Drive	

7.2 Access Control

7.2.1 Access Control

Make: HID/ Honeywell/ KABA

S. No	Specification	Complied (Yes / No)
1.	IP Rating : IP 55	
2.	Device /Reader : Proximity Reader one side/ both sides for movement	
3.	Management : Built In	
4.	Reading distance : 5-10 cm	
5.	Buzzer : Card Recognition status	
6.	Power Supply : AC/ DC	
7.	Absorbed Current : Maximum 180 Ma	
8.	Operating temperature : 0 to + 50 degree Celsius	
9.	Fixing : To wall or column	
10.	Integration : To be placed under the glass top of turnstile	
11.	Controllers : Integration with single /two door controller	
12.	Software : Readers to be connected with controllers & to be integrated with the software for generation of reports	
13.	Reports : Daily, weekly & monthly reports can be generated for attendance management	
14.	Certifications: CE Certification for the product.	

7.2.2 Flap Barrier

Make: CAME/ KABA/ Magnetic

S. No	Specification	Complied (Yes / No)
1.	Design : The design of the gate arrays should be such that the user uses the integrated reader placed inside the Barrier	
2.	Strength: The gate should be with material of enough strength for use in mass transit system.	
3.	Housing Material: Housing Material should with Arms should be of SS 304 Grade.	
4.	Power Supply : Power supply: 230V AC.	
5.	IP Rating : IP Rating- 44	
6.	Dimension : 580x 310x 950 mm (L X W X H)	
7.	Pass Speed (Minimum): 25 Person/ Min	
8.	Visual Indicators : LED indicators for signalling	
9.	Controlling : Bi- directional Electronic control with relay input contact for integration with other devices	
10.	Operating Temperature: 0 to + 50 Degree Celsius.	
11.	Relative Humidity: 95%	
12.	MCBF: 20,00,000 Cycles	
13.	Should be CE rated.	

7.2.3 Boom Barrier

Make: Magnetic/ Gunnebo/ CAME/ Brosis

S. No	Specification	Complied (Yes / No)
1.	IP Rating : IP 44 (Barrier Body) & IP 54 (Control Card Box)	
2.	Housing Material of Construction : MS Powder Coated	
3.	Protection: All Housing and internal parts will be rust & corrosion free metals or alloys of high strength with suitable Epoxy coating as applicable.	
4.	Housing Dimension (WxDxH): As per the requirement of DIT(S).	
5.	Boom Specification : Rectangular/Round	
6.	Intelligence : The barrier shall use a Hydraulic Drive in combination with microprocessor based control card communication standard interfaced Controller. It shall offer LCD Display & Graphic User Interface for easy control setting. Possibility for integration via standard user interfaces.	
7.	Loop Detector Optional Dual Loop Channel Detector	
8.	Compliance to CE.	
9.	Adherence to Safety Requirements of the • EMC Directive 2004/108/EC, • Low Voltage Directive 2006/95/EC and • The basic requirements of the Machinery • Directive 2006/42/EC	

S. No	Specification	Complied (Yes / No)
10.	Power Supply : AC/DC	
11.	Opening & Closing Time : Not More than 4 sec for 5 mtrs	
12.	Operating Temp : - 0+ 55 Degree Celsius	
13.	Safety: Detection of Presence of Vehicle in Loop or in the path of Infrared Safety Sensors available. Loops or Sensors to be used to prevent barriers from closing on the vehicle.	
14.	Duty Cycle : 100%	
15.	Integration : Shall function in integration with Smart cards, proximity reader based access control systems etc.	
16.	MCBF (Mean Cycle Between Failure): 2 Million Cycles	
17.	Certificates Required : CE / UL Certification for the product, Certification for Ingress Protection EMC Test report	

7.2.4 Work Station for Visitor Management Software

Make: HP/Dell/IBM or equivalent

S. No	Specification	Complied (Yes / No)
1.	Operating system : Operating System: Microsoft Windows 7 (32 & 64 bit), 10 (32 & 64 bit), Linux, OS X Yosemite, El Capitan	
2.	Processor : Intel Core i7 or higher	
3.	RAM : 8 GB or more	
4.	Display driver : Intel or Nvidia, 512 MB RAM or more	
5.	Disk space : 1 TB	
6.	Should have DVD+/-RW Drive	

7.3 Security Scanning

7.3.1 Baggage Scanner

Make: Smith, Rapiscan

S.No	Specification	Compliance (Yes /No)
1.	Tunnel Dimensions –600 mm (W) x 400 mm (H) (min) or more and have an Operational Weight of not more than 450kg	
2.	Conveyor Height –690 mm approx.	
3.	Conveyor belt speed should be between 0.2 / 0.24 (m/s).Conveyor movement bi-directional.	
4.	Machine should operate on 230 VAC, 50 Hz power supply and should be able to withstand voltage fluctuations in the range of 170V to 260 V. Single Phase, 3 to 5 Amp. Machine should be of Steel Construction with Steel Panels mounted on Roller Castors.	
5.	Conveyor Capacity – 165 Kg. (364 lbs) or more.	
6.	Sensors> 1152 diodes, L-shaped detector (folded array type), In case of defective diode arrays, scanning should be disabled and error message should be displayed on the screen.	
7.	X-Ray Voltage – 160 KV operating	
8.	Duty Cycle – 100%, no warm-up procedure required.	
9.	Cooling – Hermetically Sealed oil bath	
10.	The X-ray beam divergence should be such that the complete image at maximum size of bag is displayed without corner cuts. Beam divergence should be diagonal.	

S.No	Specification	Compliance (Yes /No)
11.	The radiation level should not exceed accepted health standard (0.1m R/Hr at a distance of 5 cm from external housing). Relevant certificate from AERB.	
12.	The operating temperature should be – 0 degree C to 40 degree C	
13.	Storage temperature – 20 degree C to 60 degree C.	
14.	Humidity –10%- 90% non-condensing.	
15.	Resolution: The machine should be able to display single un-insulated tinned copper wire of 40 AWG equivalent to 44 SWG. All penetration and resolution condition should be met without pressing any functional key and should be on line.	
16.	Penetration should be 35 mm thickness of steel or more.	
17.	Continuous Electronic Digital Zoom facility should be available to magnify the chosen area of an image Sixteen times (64x). Image features shall be keyboard controllable and should not be controlled using any other External device like a mouse.	
18.	Video display –19” LCD Monitor High resolution, low radiation, flicker free, resolution at least 1280 x 1024, 24 bit colour real time processing.	

S.No	Specification	Compliance (Yes /No)
19.	The machine should have features of Advanced Multi Energy X-ray imaging facility where materials of different atomic number will be displayed in different colours to distinguish between organic and inorganic materials. With this method to distinguish high-density organic materials including explosives. Machine should have variable colour or materials stripping to facilitate the operator to monitor images of organic materials for closer scrutiny. All suspicious items (Explosives, High density, material narcotics) should be displayed in one mode and that should be on line.	
20.	The machine should have the feature of selective detection of organic substances with relative atomic number numbers Zeff 7, 8, or 9. By pressing a single key it must be possible to toggle between the atomic numbers 7, 8 or 9. The image becomes a black and white image and only the image parts representing materials with the selected atomic number will be displayed in red.	
21.	The machine should have feature of automatically detecting sections of high absorption. The materials which are difficult to penetrate should be improved without deteriorating the image information of other image sections.	
22.	The machine should have the feature of warning the operator by stopping of the belt in case of presence of high absorbing material in a baggage.	

S.No	Specification	Compliance (Yes /No)
23.	Radiation Safety The machine must comply with requirements of health and safety regulations with regard to mechanical electrical and radiation hazards. Before installation of the machine, the supplier/manufacture should furnish relevant certificate from Atomic Energy Regulatory Board of India regarding radiation safety. The company manufacturing the equipment should have ISO certification for manufacturing and serving of X-ray Screening machines.	

7.3.2 Handheld Metal Detector

Make: Smith/ Ciea/Garret/Rapiscan

S.No	Specification	Compliance (Yes /No)
1.	Technology : Pulse induction technology, transmitter / receiver with automatic instant retune and should be compliant to NIJ-0602.02	
2.	Operating Frequency : 95 KHz. + 5 KHz.	
3.	Operating Voltage / current : 7 to 9 Volt DC < 50mA	
4.	Power source & endurance: Standard 9V rechargeable / disposable battery. Provided with contactless battery charger. The charger should be recharging without electrical contact.	
5.	Detection Range: Should detect a small metal object like Gem Clip from a distance of 1 inch. Instant response to all metals.	
6.	Indicators : Audio & Visual alert & vibration, Low battery indicator	
7.	Power Control : Push button / Press ON / OFF Switch	
8.	Adjustments and provisions : Provisions for adjustment of sensitivity	
9.	Safety : Safe for heart pacemakers & non-interference with magnetic recording material.	
10.	Operating Temperature : -150 C to +650 C	
11.	Protection against environmental conditions, 0 to 95% humidity	
12.	Control : Fabricated with sturdy, high impact proof, water proof, plastic. Interior circuitry should preferably be SMD component based.	
13.	Sensitivity: Minimum detection distance equal / more than 18 MM. Medium size pistol – 6 inches, Razor blade- 2 inches, Hatpin – ½ inches, Copper metal piece (05 gm)- 20 mm, Detonator (aluminium)- 30 mm, Single Al-Pin- close proximity	
14.	Battery Life: 100+ Hours continuous Service (AA NiMH batteries 2500mAh); up to 200 Hours with Automatic Sleep Mode	
15.	Technology : Pulse induction technology, transmitter / receiver with automatic instant retune and should be compliant to NIJ-0602.02	

7.3.3 Door Frame Metal Detector

Make: Smith/ Ciea/Garret/Rapiscan

S.No	Specification	Compliance (Yes /No)
1.	The equipment shall detect metal weapons carried on a person, however they are worn through the archway, independently of their orientation, trajectory and transit speed. More specifically, the equipment shall be able to detect magnetic, non-magnetic and magnetic/non-magnetic mixed alloy metal weapons singularly, assembled and/or disassembled (considering for each weapon the highest metallic contribution) or combined.	
2.	The detection capability of the WTMD shall be stable without variation. The WTMD shall not require periodic recalibration.	
3.	The sensitivity of the archway shall be adjustable in order to provide the widest dynamic threat object detection range from guns to very small blades like a half cutter blade (HCB security level).	
4.	The detection capability shall not be degraded by combinations of different types of metals	
5.	The Metal Detector shall detect the metal test pieces independently of their speed of transit through the archway (range: 0.3 … 15m/s). This requires constant sensitivity for variations in speed.	
6.	The WTMD shall be fitted with four full-height luminous bars, placed two at the entrance (right and left side) and two at the exit side of the archway (right and left side) to provide very clear visual indications according to the different conditions of the daylight.	

S.No	Specification	Compliance (Yes /No)
7.	Zone indication shall be with minimum 20 vertical floating zones for the best pinpointing of the detected metal object and the maximum resolution with a total of 60 zones (20 vertical x 3 horizontal) in the complete archway	
8.	The four multi-zone display bars shall be programmable independently as entry Stop/Go (pacing lights) indication and/or localization lights in order to improve the ergonomics and visibility of the indications and the easiness of installation.	
9.	It shall be possible to operate the WTMD in both transit directions. Pacing lights (Stop/Go indication) and/or localization lights shall be activated simultaneously on both sides of the archway.	
10.	Metal type indication: in case of alarm, the control unit shall be able to display the type of metal detected (ferrous/no ferrous). It shall be possible to enabled/disabled the metal type indication through the WTMD programming	
11.	The WTMD must have an automatic procedure for daily test activated with a Chip-card. The test result shall be displayed on the control unit.	
12.	The minimum WTMD’s passage width shall be 700 mm and the minimum WTMD’s passage height shall be 2010 mm.	
13.	The WTMD’s external dimensions shall be lower than 880 x 2300 mm (Width x Height).	
14.	The WTMD mechanical structure shall maximize the protection against wear and tear. The WTMD mechanical structure shall be very robust in order to guarantee the maximum protection against damages.	

S.No	Specification	Compliance (Yes /No)
15.	The construction of the WTMD shall be modular and designed in order to minimize the number of components	
16.	The WTMDs shall be designed in order to be assembled and disassembled quickly. The maximum allowed time for the assembling of the complete gate shall be lower than 10 minutes.	
17.	The WTMD shall be a stand-alone unit, provided with smooth, robust and washable surfaces.	
18.	The WTMD shall be equipped in the lower side with protections against damages due to bumps of floor cleaning machineries and sprinkling of water or other substances	
19.	All of the electronics shall be mounted to the crosspiece at the top of the archway.	
20.	The WTMD shall be equipped with four anchoring points to the floor.	
21.	The equipment shall have the IP65 rating for outdoor applications.	
22.	The WTMD shall be designed in order to provide the highest immunity towards external electrical and mechanical interferences in order to improve the easiness of installation in any kind of environment-layout	
23.	The correct working of the WTMD is required even when two WTMDs are installed at a reciprocal gate distance of 15 cm, without the use of synchronization cable(s) and/or jumpers.	
24.	The WTMD shall be equipped with a self diagnosis system which ensures the immediate signalling of faults or performance changes at start-up and during operation as well.	

S.No	Specification	Compliance (Yes /No)
25.	The WTMD shall be equipped with two photocells for an automatic and very high precision bidirectional counting (number of entering and exiting persons) and statistical evaluation of transiting people and alarms.	
26.	For security reasons the WTMD shall be always active. The use of photocells (infrared sensors) to avoid the alarm of the WTMD caused by nearby moving metallic materials or external electrical interferences is not allowed.	
27.	The maximum allowed power absorption of the WTMDs shall be 40W.	
28.	The WTMD shall have a minimum of five programming methods: • Chip Card • Local using Key on the control unit • Remote through a RS232 port and laptop • Infrared (IT) Remote Control (Password Protected). • Bluetooth	
29.	The selection of the security level shall be extremely quick by the use of dedicated chip-card.	
30.	The WTMD's programming access shall be protected by a mechanical lock and by a password made up of 6 alphanumeric characters. The WTMD shall have two independent levels of programming (user and super user), each one protected by a password.	

S.No	Specification	Compliance (Yes /No)
31.	The equipment shall be designed in order to improve the easiness and quickness of programming and set-up: a “one touchself installation” procedure shall be available. The self-installation procedure shall consists of a sequence of tests and adjustments, regarding the following aspects: operation of the signalling devices, relevant electrical parameters, archway configuration and the electromagnetic compatibility with the installation site (instruction for each step shall be displayed on the control unit display).	
32.	A function that searches automatically a suitable transmission channel, i.e. a channel with minimum interaction with possible sources of interference present in the installation site, shall be available. The selected transmission channel shall be shown at the end of the process.	
33.	The equipment shall be able to acquires the value of the signals received by the probe and shall adjust itself in order to increase its immunity against possible sources of interferences (environmental noise adjustment function). An additional function shall provide in the control unit display the read out of the signals measured by the probe as a percentage of the alarm threshold in order to identify a suitable detector position if the installation site contains sources of interferences.	
34.	A procedure to acquire and compensate the interferences generated by mechanical vibrations due, for instance, to floor oscillations, strong air compressions or wind shall be available.	
35.	Temperature from -20°C to +70°C.	
36.	Humidity: from 0 to 95 % without condensation	

S.No	Specification	Compliance (Yes /No)
37.	The WTMD shall be certified by an accredited and operating independent Laboratory as conforming to International Standards on the Human Exposure to Electromagnetic Fields. Manufacturer shall provide documentation.	
38.	Electrical Safety: for safety reasons, in order to avoid any probability of electrical hazard, the WTMD shall be powered by a nominal voltage to ground not exceeding 50V (CAT.0) to prevent the risk of people in transit coming into accidental contact with parts of the gate powered at mains voltage	
39.	The WTMD must use CW (continuous wave) magnetic fields (pulsed fields are not allowed) for best pace-maker and vital supports harmlessness.	
40.	The WTMD shall not interfere with medical devices such as hearing aids, cardiac stimulators, defibrillators, neurological stimulators.	

7.4 Networking and Infrastructure

7.4.1 Network Monitoring System

Make: HP/ CA/ Solar winds/WhtsupGold

S. No	Specification	Complied (Yes / No)
1.	The system should provide a scalable network management solution with advanced fault and performance management functionality across critical IT resources viz. Routers, Switches, Firewalls, WAN links, IT infrastructure components.	
2.	Automatic detection of nodes in the network across layer 2 and layer 3; including the functionality of the nodes	
3.	The system should be able to detect the network topology and also be able to map them geographically	
4.	Actively monitor any vendor device in the network using WMI, Telnet, and SSH, or by any custom script.	
5.	It should report the status of network nodes; including the discovery of any new nodes.	
6.	Manage any node with standard and enterprise management information base (MIB) objects	
7.	Proactively monitor the availability of the nodes along with their system resources such as, CPU, memory and temperature	
8.	Actively monitor switch ports and notify any port events. It should be able to identify all devices connected to a port.	

S. No	Specification	Complied (Yes / No)
9.	It should support the following protocols • SNMP v2 and v3 • TCP/IP • IPX/DMI • ICMP • ARP/RARP • WMI	
10.	It should provide reports on performance, availability, logs and events on a customizable fashion	
11.	Flow based network traffic analysis to generate reports on which user, application, source, destination or conversation is using the bandwidth.	
12.	Bandwidth utilization report on the basis of real-time, hourly, daily, weekly, monthly and yearly	
13.	Reports of Network interfaces, switch port availability and alerts on traffic thresholds	
14.	The system should capture Sys logs, Windows event logging and SNMP traps to identify any faults. It should alert the network administrator either by email	
15.	It should have the capability to display the alerts on a central console (say a TV/big display) with customizable dashboards.	

S. No	Specification	Complied (Yes / No)
16.	SNMP MIB Browser to walk through specific MIBs to identify any faults. Define event thresholds for MIB objects.	
17.	The system should monitor WAN links, bandwidth utilization and round-trip-time (RTT) for any early detection of network outages or performance. It should be able to visualize the WAN links performance (including latency) and help in identifying any potential problems	
18.	NMS should be scalable to manage up to 300 devices	
19.	It should have the capability to run 24x7 with a hot-standby failover functionality	
20.	Automate policy-based change, configuration and compliance of network devices.	
21.	Security audit report of user and administration logging and configurations along with time stamps.	

7.4.2 Layer 3 Switch (24 Port)

Make: **Cisco/ Juniper/ Brocade**

Sl. No.	Specifications	Complied (Yes / No)
1.	Switch capacity - 1.4 Tbps or higher	
2.	Switch forwarding rates – 1Bpps or higher	
3.	10G/Gigabit - 24 ports SFP and / or SFP+	
4.	Non-blocking switch architecture and modular operating system	
5.	802.3ad based standard port/link aggregation, Jumbo frames, storm control	
6.	Support at least 4000 VLAN and 150,000 MAC Address	
7.	802.1X Network Security and Radius/TACACS AAA authentication	
8.	MAC Address filtering based on source and destination address	
9.	support for various ACLs like port based, vlan based and L2- L4 ACL's	
10.	Should have Control plane (DoS) protection	
11.	The switch should support MACsec, SSH v1 & v2 and Dynamic ARP inspection	
12.	Layer3 routing protocols like Static, RIP, OSPF, RIPnG, OSPFv3 from day 1 for the solution.	
13.	The switch should support MPLS, L2 and L3 VPN and IPv6 Tunneling	
14.	8 number of hardware queues per port	
15.	DSCP, 802.1p	
16.	IGMP v1,v2,v3, IGMP snooping, PIM SM and MSDP	

Sl. No.	Specifications	Complied (Yes / No)
17.	The switch should support ISSU and BFD	
18.	SNMP v1, v2, v3, RMON/RMON-II enabled, SSH, telnet, GUI, Web management and should have dedicated Management port	
19.	The switch should support CLI via console, telnet, or SSH and should have image rollback option.	
20.	Switch should support port mirroring feature for monitoring network traffic of a particular port/VLAN.	
21.	Switch should support Link Aggregation on two different switches	
22.	Built-in real-time performance monitoring capabilities	
23.	Power Supply: Switch should have internal Hot Swappable Redundant Power supply	
24.	Cooling Fans: Should have redundant cooling FANS	
25.	The switch should support NEBS	
26.	Switch should be stackable/VPC/Equivalent (All accessories to be provided from day 1)	
27.	The Switch should be EAL3/ NDPP certified	

7.4.3 Layer 2 Switch with POE

Make: Cisco/ Juniper/ Brocade

S. No	Specification	Complied (Yes / No)
1.	Minimum 24 ports of 10/100/1000 base-T PoE and 2 additional SFP uplink ports	
2.	1 U Rack mountable and should support stacking	
3.	52 Gbps or higher Backplane capacity and minimum 38 Mpps of forwarding rate	
4.	Should support Non-blocking and distributed forwarding hardware architecture	
5.	All interfaces should provide wire speed forwarding for both Fiber and copper modules	
6.	Support for at least 1000 VLANs & 16k MAC address	
7.	It should have static IP routing and RIP	
8.	Switch should support 8 hardware queues per port	
9.	Dynamic Host Configuration Protocol (DHCP) snooping	
10.	Switch should support LLDP and LLDP-MED capabilities	
11.	Should support IP source guard & DAI	
12.	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).	
13.	Switch needs to have console port for administration & management	
14.	Management using CLI, GUI using Web interface should be supported	
15.	FTP/TFTP for upgrading the operating System	
16.	IEEE 802.1x support	
17.	IEEE 802.1D Spanning-Tree Protocol	

S. No	Specification	Complied (Yes / No)
18.	IEEE 802.1p class-of-service (CoS) prioritization	
19.	IEEE 802.1Q VLAN	
20.	IEEE 802.3 10BASE-T specification	
21.	IEEE 802.3u 100BASE-TX specification	
22.	IEEE 802.3af	
23.	IEEE 802.3at	
24.	Switch should able to support management via CLI, Web interface	
25.	SNMP v1,v2,v3	
26.	Switch should be manageable through both IPv4 & IPv6.	
27.	Switch should be UL-UL60950-1, EN 55022 Class A, CE	
28.	Should have modular OS and should support configuration roll back to recover mis-configured switch to last known good configuration	
29.	The switch should be EAL 3/NDPP certified under Common Criteria.	

7.4.4 42 U RACK

Make: APW, Rital. MTS

S.No	Specification	Compliance (Yes /No)
1	19 " Rack , Floor mount min 600 mm depth, 42 U height, Front glass door (lockable, toughened 4mm),	
2	19 " mountable ,1U , Universal power socket design to fit both round & flat socket with built in surge protection & over load circuit breaker	
3	5 AMP AC power distribution channel made of high flame retardant & insulating material , CE approved with 6 no's sockets (5 no's) , with wall mounting hardware	
4	Copper earthing kit (19" copper bar) & equipment mounting screws/hardware packets (2 no's)	
5	Fan tray with two fans (low noise, good quality, ball bearing type ,90 CFM)	
6	Surface Finish: EC Dip Coat Primed and Powder Coated to 80-100microns with RAL 7035 Light Grey	
7	Should confirm To DIN 41494 & IEC 297 standard , Load bearing capacity of 100 Kgs	
8	Castors with brakes	

7.4.5 9 U RACK

Make: APW, Rital. MTS

S.No	Specification	Compliance (Yes /No)
1	19 " Rack , Floor mount min 600 mm depth, 9 U height, Front glass door (lockable, toughened 4mm),	
2	19 " mountable ,1U , Universal power socket design to fit both round & flat socket with built in surge protection & over load circuit breaker	
3	5 AMP AC power distribution channel made of high flame retardant & insulating material, CE approved with 6 no's sockets (2 no's) , with wall mounting hardware	
4	Copper earthing kit (19" copper bar) & equipment mounting screws/hardware packets (2 no's)	
5	Fan tray with two fans (low noise, good quality, ball bearing type ,90 CFM)	
6	Surface Finish: EC Dip Coat Primed and Powder Coated to 80-100microns with RAL 7035 Light Grey	
7	Should confirm To DIN 41494 & IEC 297 standard , Load bearing capacity of 50 Kgs	

7.4.6 CAT 6 UTP Cable

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Category 6 Unshielded Twisted Pair 100W cable shall be compliant with EIA/TIA 568-C.2 transmission performance specifications.	
2	Category 6 UTP cables shall extend between the work area location and its associated telecommunications closet and consist of 4 pair, 23 AWG, UTP Non Plenum cable jacket	
3	The 4 pair Unshielded Twisted Pair cable shall be ULÒ Listed	
4	Construction: 4 twisted pairs separated by internal X shaped, 4 channel, polymer spine / full separator. Half shall not be accepted.	
5	Conductor: Solid Copper	
6	Conductor Diameter: 0.57±0.005mm (23 AWG only).	
7	Insulator Polyolefin.	
8	Jacket: PVC, BLUE in color.	
9	Outer Diameter: 6.0±0.4mm	
10	Insulation Dia. (±0.05mm): 1.04.	

7.4.7 Jack Panel

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Be made of cold rolled steel, in 24 port configurations. Each jack should have spring loaded shutter inside the jack for 100% dust free environment.	
2	Allow for a minimum of 750 plug mating cycles.	
3	Panel Size should be 1 U only.	
4	Should individually replaceable I/Os	
5	I/Oscolor should be back only for Jack Panel	
6	Have port identification numbers on the front of the panel.	
7	Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, with optional color labels / icons.	
8	Each port / jack on the panel should be individually removable on field from the panel.	
9	Should have integrated rear cable management shelf (Cable support Bar). • Should comply to the following : TIA/EIA-568-C.2 Component Compliant • FCC Subpart F 68.5 Compliant • IEC-603-7 Compliant • ISO 11801 Class E Compliant • UL 1863 • ETL Verified & UL Listed.	

7.4.8 Information Outlet

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Category 6, EIA/TIA 568-C.2 – 250MHz.	
2	Information outlets should have ETL component compliance (ETL certificate to be enclosed) Report.	
3	All information outlets for 100 W, 22-24 AWG copper cable shall: Use insulation displacement connectors (IDC).	
4	Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limits.	
5	Be constructed of high impact, flame-retardant thermoplastic with color and icon options for better visual identification.	
6	Should have spring loaded integrated shutter.	
7	Should have Terminator cap.	
8	IDC posts should be pointed	

7.4.9 Patch Cords

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Category 6 Equipment cords	
2	The work area equipment cords shall, at a minimum comply with proposed ANSI/TIA/EIA-568-C.2 Commercial Building Cabling Standards Transmission Performance Specifications for 4 pair 100W Category 6 Cabling.	
3	Category 6 modular equipment cords: Shall be round, and consist of eight insulated 24 AWG, stranded copper conductors, arranged in four color-coded twisted-pairs	
4	Equipped with modular 8-position plugs on both ends, wired straight through with standards compliant wiring.	
5	Should have 50 micro inches of gold plating over nickel contacts.	
6	Modular cords should include slim clear anti-snag slip-on boots	
7	Mounting cords should have ETL component compliance. (ETL certificate to be enclosed).	
8	Conductor size: 24 AWG stranded bare copper.	
9	Nominal outer diameter: 5.9mm.	
10	Jacket: LSOH / LSZH.	
11	Temperature range: - 20°C to + 60°C.	
12	Operating life: Minimum 750 insertion cycles.	

S. No	**Specification**	**Complied (Yes / No)**
13	Contact material: Copper alloy.	
14	Contact plating: 50µ” Gold/100µ”Nickel.	
15	Plug dimensions compliant with ISO/IEC 60603-7-4 and FCC 47 Part 68	
16	Fire Propagation tests: LS0H Sheath: CSA FT1, IEC 60332-1, IEC 61034	
17	Max voltage: 150 VAC (max).	
18	Max current: 1.5A @ 25°C.	

7.4.10 Face Plate

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Dual square plate, 86mmx86mm	
2	Write on labels in transparent plastic window – supplied with plate	
3	Screw hole covers – to be supplied with plate	
4	Plug in Icons – Icon tree – to be supplied with plate	
5	Without dustcover	
6	Should be able to support variety of jacks – UTP, STP, Fiber, Coax etc.	

7.4.11 Optical Fiber Cable Armored Multi Mode 6 Core

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	No of Cores :6	
3	Tube Identification: Single tube	
4	Fiber protection(Tube): Polybutylene Terephthalate (PBT)	
5	Water Blocking: Thixotropic Gel (Tube) and Petroleum Jelly (Interstices)	
6	Core Wrapping: Polyethylene Terephthalate	
7	Armouring: Corrugated Steel Tape Armour (ECCS Tape)	
8	Sheath: LSZH Sheath Black ;IEC 60332-1 Complied LSZH with fire retardant properties	
9	Max. Tensile Strength-Short Term: 1500N	
10	Max. Crush Resistance-Short Term: 2000N/10 cm	
11	Mass: 95 kg/km minimum	
12	Attenuation at 850 nm-3.5 dB/km and at 1300 nm: 1.5 dB/km	
13	Specifications: ISO.IEC 11801 - 2nd Edition, type OM4; AS/ACIF S008; AS/NZS 3080; LSZH specifications.	

7.4.12 Patch Panel 12/24 Port

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Have sufficient slots accommodate duplex SC adapters individually.	
2	Should have fiber management provision inside.	
3	Have earthing lugs and other accessories.	
4	Provide self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, for front panel labelling.	
5	Fiber panel should be capable of both Rack as well as wall mountable	

7.4.13 SC Duplex Adaptor

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	All SC adaptors should be duplex type Multimode.	
2	Adapters should be snap mount for easy insertion and removal.	
3	Should have integrated shutter for protection against dust	

7.4.14 Fiber Pigtails

Make: Molex/Panduit/Corning/ Schneider/ Tyco

S. No	Specification	Complied (Yes / No)
1	Precision ferrule endface geometry	
2	Factory polished, tested and serialized.	
3	Buffer Diameter: 900um tight buffer	
4	Minimum bend radius: install: 30 mm	
5	Retention Strength: 100N	
6	Cable: 900um Buffered	
7	SC type Single	
8	Sheath :LSZH	

8. Service Level Requirement and Targets

The SLAs have been logically segregated in the following categories:

(a) Pre Implementation

(b) Post Implementation (Maintenance period)

8.1 Pre Implementation SLA and associated Penalties

The below measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract.

Project Activities	**Baseline Timeline (in Months) T= Date of signing of Contract**	**Penalty**
Site Survey report & Final BOM to be submitted	T+1	@INR 5,000/- per week delay
Delivery of Hardware and Software in DIT(S)	T+2	@INR 10,000/-per week delay
Installation and commissioning of the required Hardware and Software at DIT(S)	T+4	@INR 25,000/- per week delay

8.2 Post Implementation SLA

Ref	Service Description	Service Level	Method of calculating service delivery
SLA 01	**Manpower availability:** Adequate number of manpower must be deployed in each shift for managing operations on day to day basis. Manpower availability shall also measure the availability of the required skill sets as proposed by the SI in its proposal in respect of Key Personnel in Volume 1 of the RFP. In case of replacements, the new resource should be of similar or higher skill set.	The manpower deployed should adhere to the RFP requirements	All deviations would be recorded and MIS report shall be made available to DIT(S).

Ref	Service Description	Service Level	Method of calculating service delivery
SLA 02	**Recording and Reporting of Faults:** The malfunctions of CCTV Surveillance, Access Control and Security Scanning System etc. by any reason whatsoever must be recorded and reported.	Comprehensive recording and reporting of all faults should be provided to DIT(S). Report needs to cover incident type, service impact, resolution timescale, likelihood of repetition. Comprehensive report must be produced within 10 days of the end of the reporting month. However, a summarized report specifying the fault shall be submitted to DIT(S) at the end of day on which fault has occurred.	Log Book
SLA 03	**CCTV Camera Fault** – CCTV Cameras should be fixed or replaced within 24 hours. **Other faults:** SI shall ensure that any other fault is attended within 4 hours after DIT(S) log a call for the failure or SI comes to know about the failure.	The SI must hold stocks of all parts and wherever necessary complete replacements. All the complaints received after 05:00 P.M. must be attended by 11:00 A.M. on the next day.	Log Book

Ref	Service Description	Service Level	Method of calculating service delivery
SLA 04	**Uptime**	The SI should ensure to achieve uptime of 98.5% of the scheduled operating time as defined in Schedule I of volume 2 of this RFP.	Log Book
SLA 05	**Information Requests** - All information requests by the authorized DIT(S) Officer shall be considered on receipt. Data is normally held for 30 days therefore if a request is received on day 29 back up footage will have to be requested immediately to fulfil the request.	All requests to be responded to within 24 hours. However, all requests must be reviewed and considered on the day of receipt or on the next Working Day if received after 5.00 P.M.	Log Book
SLA 06	**Obtaining Evidence** - Evidence copied for law enforcement agencies and other authorized third parties	Evidence to be provided after due approval of DIT(S).	Log Book

All the SLA and penalty calculation will be done manually on the basis of complaints/tickets logged at the Monitoring center. Post validation yearly payments may be released after deducting appropriate amount of penalty.

8.3 Calculation of Penalty:

S.No.	Service Level	Weightage (out of 10)
1.	SLA 01	2
2.	SLA 02	2
3.	SLA 03	2
4.	SLA 04	2
5.	SLA 05	1
6.	SLA 06	1

i) The weightage against respective SLA shall be added for every breach in service level. If the total weightage of all the Service Levels breaches 80% marking (i.e. 8 out of 10) in each of the in two consecutive months then penalty @ Rs. 2,000/- (Rs. Two thousand only) may be levied.

ii) Further, in case of more than 3 breaches (not continuous) of 80% marking in two successive quarters then again penalty @ Rs. 5,000/- (Rs. Five Thousand Only) may be levied.

iii) Upon breach of Service Levels for a continuous period of 3 months, DIT(S) may terminate the contract as per provisions of section 2.19 of volume 2 of the RFP.

8.4 Acceptance Testing and Certification

i) The primary goal of Acceptance Testing and Certification is to ensure that the Project (including all the project components as discussed in the scope of work) meets requirements, standards, specifications and performance, by ensuring that the following are associated with clear, quantifiable metrics for accountability:

a. Functional requirements

b. Infrastructure (Hardware and Network) Compliance Review

c. Availability of the project Services in the defined locations

d. Performance

e. Security

f. Manageability

g. A Reporting System

h. Project Documentation (Design, development, configuration, training and administration manuals etc.)

ii) As part of Acceptance testing, performed through a third party agency, DIT(S) shall review all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement.

iii) The procedures and parameters for testing, may be laid down by the Third Party Agency or by DIT(S); the solution deployed by the vendor has to satisfy third party or DIT(S), upon which the system shall go-live.

iv) DIT(S) will establish appropriate processes for notifying the selected SI of any shortcomings from defined requirements at the earliest instance after noticing the same to enable the selected SI to take corrective action. All gaps identified shall be addressed by the vendor immediately prior to Go-live of the solution. It is the responsibility of the selected SI to take any corrective action required to remove all shortcomings, before the roll out of the project.

v) It is to be noted that the involvement of the third party for acceptance testing and certification, does not absolve the vendor of his responsibilities to meet all SLAs as laid out in this RFP document.

vi) It is to be noted that:

- DIT(S) may get the solution audited through a Third Party or by DIT(S) office itself; before Go-Live and periodically after Go-Live in order to ensure the success of the project.

Following discusses the acceptance criteria to be adopted for the project as mentioned above. The list below is indicative and the activities will include but not be limited to the following:

8.5 Functional Requirement Review

i) The solution developed/customized by selected Bidder shall be reviewed and verified by the agency against the Functional Requirements signed-off between the DIT(S) and the selected Bidder. All gaps, identified shall be addressed by the vendor immediately prior to Go-live of the solution.

ii) One of the key inputs for this testing shall be the traceability matrix to be developed by the vendor for the solution. Apart from Traceability Matrix, agency may develop its own testing plans for validation of compliance of system against the defined requirements.

iii) The acceptance testing w.r.t. the functional requirements shall be performed by independent third party agency (external audit) as well as the select internal department users (User Acceptance Testing) and system has to satisfy both third party acceptance testing and internal user acceptance testing, upon which the system shall go-live.

8.6 Infrastructure Compliance Review

DIT(S) or its nominated third party agency shall perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure (both IT, non IT as well as Network infrastructure) supplied by the selected SI against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by the selected SI. Compliance review shall not absolve the SI from ensuring that proposed infrastructure meets the SLA requirements.

8.7 Security Review

The CCTV Solution Deployed shall be audited by the DIT(S) officials or its nominated third party agency from a security and controls perspective. Such audit shall also include the IT infrastructure and network deployed for the project. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the solution to the following activities.

(i) Audit of Network, Server and Surveillance security mechanisms

(ii) Assessment of authentication mechanism provided in the components/modules

Assessment of data access privileges, retention periods and archival mechanisms

8.8 Performance

Performance is another key requirement for the project and the agency shall review the performance of the deployed solution against certain key parameters defined in SLA. Such parameters include request-response time, work-flow processing time, concurrent sessions supported by the system etc., Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the solution for catering to the project requirements.

8.9 Availability

The solution should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including network, server, surveillance security, fail-over tests to verify the availability of the services in case of component failures. The agency shall also verify the availability of the project services to all the users in the defined locations.

8.10 Manageability Review

The agency shall verify the manageability of the solution and its supporting infrastructure deployed using the Network Management System (NMS) proposed by the selected Bidder. The manageability requirements include requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc.

8.11 SLA Reporting System

The selected SI shall design, implement/customize the Network Management System (NMS) for the project and shall develop any additional tools required to monitor the performance indicators listed as per the SLAs mentioned the RFP. The Acceptance Testing and Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the vendor and shall certify the same. The NMS deployed for the project, based on SLAs, shall be configured by the selected SI to calculate the payment to be paid by the department after deducting the necessary penalties.

8.12 Project Documentation

DIT(S) or its nominated third party agency shall review the project documents developed by the selected SI including requirements, design, installation and administration manuals, version control etc. Any issues/gaps identified, in any of the above areas, shall be addressed to the complete satisfaction of the DIT(S)

9. NON-DISCLOSURE AGREEMENT

THIS AGREEMENT is made on this the <***> day of <***> 20--- at <***>, India.

BETWEEN

--- having its office at -- India hereinafter referred to as '**DIT(S)**' or '----------------‘, which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as '**the System Integrator/SI**' which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'.

WHEREAS:

1. DIT(S) is desirous for Implementation and Operations Management of “CCTV Surveillance, Access Control & Security Scanning system”.
2. DIT(S) and SI have entered into a Master Services Agreement dated <***> (the “MSA”) in furtherance of the Project.
3. Whereas in pursuing the Project (the “**Business Purpose**”), a Party (“Disclosing Party) recognizes that they will disclose certain Confidential Information (as defined hereinafter) to the other Party (“Receiving Party”).
4. Whereas such Confidential Information (as defined hereinafter) belongs to Receiving Party as the case may be and is being transferred to the Disclosing Party to be used only for the Business Purpose and hence there is a need to protect such information from unauthorized use and disclosure.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

DEFINITIONS AND INTERPRETATION

9.1 Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the same meanings set out in Schedule I of MSA.

9.2 Interpretation

In this Agreement, unless otherwise specified:

(i) references to Clauses, Sub-Clauses, Paragraphs and Schedules are to clauses, sub-clauses, paragraphs of and schedules to this Agreement;

(ii) use of any gender includes the other genders;

(iii) references to a ‘company’ shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

(iv) references to a ‘person’ shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

(v) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;

(vi) any reference to a ‘day’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;

(vii) references to a ’business day’ shall be construed as a reference to a day (other than Saturday, Sunday and other gazetted holidays) on which DIT(S) is generally open for business;

(viii) references to times are to Indian standard time;

(ix) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

(x) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

9.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

9.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

(a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

(b) as between the provisions of this Agreement and the Schedules, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules; and

(c) as between any value written in numerals and that in words, the value in words shall prevail.

9.5 Priority of Agreements

The Parties hereby expressly agree that for the purpose of giving full and proper effect to this Agreement, the MSA and this Agreement shall be read together and construed harmoniously. In the event of any conflict between the MSA and this Agreement, the provisions contained in the MSA shall prevail over this Agreement.

9.6 Term

This Agreement will remain in effect for five years from the date of the last disclosure of Confidential Information ("***Term***"), at which time it will terminate, unless extended by the disclosing party in writing.

9.7 Scope of the Agreement

(a) This Agreement shall apply to all confidential and proprietary information disclosed by Disclosing Party to the Receiving Party and other information which the disclosing party identifies in writing or otherwise as confidential before or within (30) thirty days after disclosure to the Receiving Party ("Confidential Information"). Such Confidential Information consists of certain specifications, documents, software, prototypes and/or technical information, and all copies and derivatives containing such Information that may be disclosed to the Disclosing Party for and during the Business Purpose, which a party considers proprietary or confidential.

(b) Such Confidential Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to the Receiving Party.

9.8 Obligations of the Receiving Party

The Receiving Party shall:

(a) use the Confidential Information only for the Business Purpose and shall hold the Confidential Information in confidence using the same degree of care as it normally exercises to protect its own proprietary information, taking into account the nature of the Confidential Information, and

(b) grant access to Confidential Information only to its employees on a “need to know basis‟ and restrict such access as and when not necessary to carry out the Business Purpose.

(c) cause its employees to comply with the provisions of this Agreement;

(d) reproduce Confidential Information only to the extent essential to fulfilling the Business Purpose, and

(e) prevent disclosure of Confidential Information to third parties;

(f) disclose the Confidential Information to its consultants/contractors on a need to know basis; provided that by doing so, the Receiving Party agrees to bind such consultants/ contractors to terms at least as restrictive as those stated herein. The Receiving Party upon making a disclosure under this Clause shall:

   (i) advise the consultants/contractors of the confidentiality obligations imposed on them by this Clause.

(g) upon the Disclosing Party's request, the Receiving Party shall either return to the disclosing party all Confidential Information or shall certify to the disclosing party that all media containing Confidential Information have been destroyed. Provided, however, that an archival copy of the Confidential Information may be retained in the files of the Receiving Party's counsel, solely for the purpose of proving the contents of the Confidential Information.

(h) not to remove any of the other Party's Confidential Information from the premises of the Disclosing Party without prior written approval.

(i) exercise extreme care in protecting the confidentiality of any Confidential Information which is removed, only with the Disclosing Party's prior written approval, from the Disclosing Party's premises. Each Party agrees to comply with any and all terms and conditions the disclosing party may impose upon any such approved removal, such as conditions that the removed Confidential Information and all copies must be returned by a certain date, and that no copies are to be made off of the premises.

(j) Upon the Disclosing Party's request, the Receiving Party shall promptly return to the Disclosing Party all tangible items containing or consisting of the disclosing party's Confidential Information all copies thereof.

9.9 Exceptions to Confidential Information

The foregoing restrictions on each party's use or disclosure of Confidential Information shall not apply to the Confidential Information that the Receiving Party can demonstrate that such Confidential Information:

(a) was independently developed by or for the Receiving Party without reference to the Information, or was received without restrictions; or

(b) has become generally available to the public without breach of confidentiality obligations of the Receiving Party; or

(c) was in the Receiving Party's possession without restriction or was known by the Receiving Party without restriction at the time of disclosure; or

(d) is the subject of a subpoena or other legal or administrative demand for disclosure; provided, however, that the Receiving Party has given the disclosing party prompt notice of such demand for disclosure and the Receiving Party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order; or

(e) is disclosed with the prior consent of the disclosing party; or

(f) was in its possession or known to it by being in its use or being recorded in its files or computers or other recording media prior to receipt from the disclosing party and was not previously acquired by the Receiving Party from the disclosing party under an obligation of confidence; or

(g) the Receiving Party obtains or has available from a source other than the disclosing party without breach by the Receiving Party or such source of any obligation of confidentiality or non-use towards the disclosing party.

9.10 Ownership of the Confidential Information

(a) Each Party recognizes and agrees that all of the disclosing Party’s Confidential Information is owned solely by the Disclosing Party (or its licensors) and that the unauthorized disclosure or use of such Confidential Information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain.

(b) By disclosing the Confidential Information or executing this Agreement, Disclosing Party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right. The Disclosing Party disclaims all warranties regarding the information, including all warranties with respect to infringement of intellectual property rights and all warranties as to the accuracy or utility of such information.

(c) Access to Confidential Information hereunder shall not preclude an individual who has seen such Confidential Information for the purposes of this Agreement from working on future projects for the Disclosing Party which relate to similar subject matters, provided that such individual does not make reference to the Confidential Information and does not copy the substance of the Confidential Information during the Term. Furthermore, nothing contained herein shall be construed as imposing any restriction on the Receiving Party's disclosure or use of any general learning, skills or know-how developed by the Receiving Party's personnel under this Agreement.

(d) Execution of this Agreement and the disclosure of Confidential Information pursuant to this Agreement do not constitute or imply any commitment, promise, or inducement by either Party to make any purchase or sale, or to enter into any additional agreement of any kind.

9.11 Dispute Resolution

(a) If a dispute arises in relation to the conduct of this Contract (Dispute), a party must comply with this clause 9.11 before starting arbitration or court proceedings (except proceedings for urgent interlocutory relief). After a party has sought or obtained any urgent interlocutory relief that party must follow this clause 9.14.

(b) A party claiming a Dispute has arisen must give the other parties to the Dispute notice setting out details of the Dispute.

(c) During the 14 days after a notice is given under clause 9.11 (b) (or longer period if the parties to the Dispute agree in writing), each party to the Dispute must use its reasonable efforts through a meeting of Senior Executive (or their nominees) to resolve the Dispute. If the parties cannot resolve the Dispute within that period then any such dispute or difference whatsoever arising between the parties to this Contract out of or relating to the construction, meaning, scope, operation or effect of this Contract or the validity of the breach thereof shall be referred to a sole arbitrator to be appointed by mutual consent of both the parties herein. If the parties cannot agree on the appointment of the arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then the Arbitrator shall be appointed by the High Court of Delhi. The provisions of the Arbitration and Conciliation Act, 1996 will 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 arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules or re-enactments thereof.

(d) The Receiving Party agrees that the Disclosing Party shall have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.

9.12 Variation

This Agreement may only be varied in writing and signed by both Parties.

9.13 Waiver

Waiver including partial or conditional waiver, by either Party of any default by the other Party in the observance and performance of any provision of or obligations under this Agreement:-

(a) shall be in writing

(b) shall not operate or be construed as a waiver of any other or subsequent default hereof or of other provisions of or obligations under this Agreement;

(c) shall be executed by a duly authorized representative of the Party; and

(d) shall not affect the validity or enforceability of this Agreement in any manner.

9.14 Exclusion of Implied Warranties

This Agreement expressly excludes any warranty, condition or other undertaking implied at law or by custom or otherwise arising out of any other agreement between the Parties or any representation by either Party not contained in a binding legal agreement executed by both Parties.

9.15 Entire Agreement

This Agreement and the Annexure together constitute a complete and exclusive statement of the terms of the agreement between the Parties on the subject hereof, and no amendment or modification hereto shall be valid and effective unless such modification or amendment is agreed to in writing by the Parties and duly executed by persons especially empowered in this behalf by the respective Parties. All prior written or oral understandings, offers or other communications of every kind pertaining to this Agreement are abrogated and withdrawn.

9.16 Severability

If for any reason whatever, any provision of this Agreement is or becomes invalid, illegal or unenforceable or is declared by any court of competent jurisdiction or any other instrumentality to be invalid, illegal or unenforceable, the validity, legality or enforceability of the remaining provisions shall not be affected in any manner, and the Parties shall negotiate in good faith with a view to agreeing to one or more provisions which may be substituted for such invalid, unenforceable or illegal provisions, as nearly as is practicable to such invalid, illegal or unenforceable provision. Failure to agree upon any such provisions shall not be subject to the dispute resolution procedure set forth under this Agreement or otherwise.

9.17 No Partnership

This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the Parties, or to impose any partnership obligation or liability upon either Party, and neither Party shall have any right, power or authority to enter into any agreement or undertaking for, or act on behalf of, or to act as or be an agent or representative of, or to otherwise bind, the other Party except as expressly provided under the terms of this Agreement.

9.18 Third Parties

This Agreement is intended solely for the benefit of the Parties and their respective successors and permitted assigns, and nothing in this Agreement shall be construed to create any duty to, standard of care with reference to, or any liability to, any person not a Party to this Agreement.

9.19 Successors and Assigns

The Agreement shall be binding on and shall inure to the benefit of the Parties and their respective successors and permitted assigns.

9.20 Notices

Any notice or other communication to be given by any Party to the other Party under or in connection with the matters contemplated by this Agreement shall be in writing and shall be given by hand delivery, recognized courier, registered post, email or facsimile transmission and delivered or transmitted to the Parties at their respective addresses set forth below:

If to DIT(S):

Attn: <***>

Tel:

Fax:

Email:

Contact:

With a copy to:

If to the System Integrator:

Attn. <***>

Phone: <***>

Fax No. <***>

9.21 Language

All notices required to be given by one Party to the other Party and all other communications, documentation and proceedings which are in any way relevant to this Agreement shall be in writing and in the English language.

9.22 Counterparts

This Agreement may be executed in counterparts, each of which, when executed and delivered, shall constitute an original of this Agreement.

9.23 Mitigation

Without prejudice to any express provisions of this Agreement on any mitigation obligations of the Parties, each of DIT(S) and the SI shall at all times take all reasonable steps to minimize and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to this Agreement.

9.24 Removal of Difficulties

The Parties acknowledge that it is conceivable that the Parties may encounter difficulties or problems in the course of implementation of the Project and the transactions envisaged under this Agreement. The Parties agree and covenant that they shall mutually discuss such difficulties and problems in good faith and take all reasonable steps necessary for removal or resolution of such difficulties or problems.

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED

For and on behalf of the Implementation

Agency by: DIT(S)

SIGNED, SEALED AND DELIVERED

For and on behalf of the Nodal

Agency by:

(Signature)	(Signature)
(Name): Shri. Sanjeev Singh	(Name)
(Designation): Additional Director	
General (Systems) – 2	(Designation)
(Address) Aayakar Bhawan, Vaishali,	
Ghaziabad - 201010	(Address)
(Fax No.) 0120-2770452	(Fax No.)

In the presence of:

1.

2.

10. Integrity Pact

General

This Agreement (hereinafter called the Integrity Pact) is made on _____ day of the month of _____ 20___, between, on one hand, the President of India acting through Additional Director General of Income Tax (Systems) – 2, Directorate of Income Tax(Systems), Central Board of Direct Taxes, Department of Revenue, Ministry of Finance , Government of India (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s _________________________ represented by ______________________________________, Chief Executive Officer / Authorized Signatory (hereinafter called the "BIDDER/Seller", which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to engage the Service Integrator (SI) for Supply, Installation, Commissioning & Maintenance of "CCTV Surveillance, Access Control & Security Scanning System" at Aayakar Bhawan, Vaishali, Ghaziabad and the BIDDER is willing to offer/has offered the services and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Ministry/Department of the Government of India performing its functions on behalf of the President of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

Enabling the BUYER to obtain the desired services at a competitive price in conformity with the defined specification by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organisation or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all the BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

Commitments of the BIDDERs

3. The BIDDER commits itself to take all the measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour or any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.

3.3 BIDDER shall disclose the name and address of agents and representatives and Indian BIDDER shall disclose their foreign principals and associates.

3.4 BIDDER shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the BIDDER who is involved in the bid process or any employee of such BIDDER or any person acting on behalf of such BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of BUYER who is involved in the bid process has financial interest/stake in the BIDDER’s firm, the same shall be disclosed by the BIDDER at the time of filing of tender.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount __________ as specified in the RFP as Earnest Money/Security Deposit, with the BUYER through any of the following instruments:

(i) Bank Draft or a Pay Order in favour of __________
(ii) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.
(iii) Any other mode or through any other instrument, as stated in RFP.

5.2 The EMD of Rs. 10,00,000/- deposited along with the Bid shall remain valid till the submission of performance guarantee by the BIDDER.

5.3 In case of the successful BIDDER, a clause would also be incorporated in the Performance Bank Guarantee that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 Within 15 days of the receipt of notification of award from the Employer, the successful Bidder shall furnish the performance security equal to 10% of the value of contract from a Nationalized / Scheduled Bank in accordance with the General Conditions of Contract, in the proforma prescribed at Form 8 of Volume – I of the RFP.

5.5 Performance Security should remain valid for a period of sixty days beyond the date of completion of all contractual obligations including warranty obligations.

5.6 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/ Performance Security for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:-

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Performance Security (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be require to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

(iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilised to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.

(viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.

(x) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1 (i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

7.1 The BIDDER undertakes that under similar buying conditions, it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or subsystems was so supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 Shri Samirendra Chatterjee, IAS(Retd.) has been appointed as Independent External Monitor (hereinafter referred to as Monitor) for overseeing and implementation of the Pre-Contract Integrity Pact for procurement of services in the Department of Revenue. His contact details are as under:

Shri Samirendra Chatterjee, IAS (Retd.)

71, Vikramshila Apartment

IIT Delhi Campus

HauzKhas

New Delhi -110016

Mob no. 9911158262

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is New Delhi.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto a period of five years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later.

12.2 The complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later, in case BIDDER is unsuccessful, this integrity Pact shall expire after six months from the date of the signing of the contract.

12.3 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at ________________ on ______________

BUYER	BIDDER
Shri Sanjeev Singh	CHIEF EXECUTIVE OFFICER / AUTHORIOZED SIGNATORY

Additional Director General (Systems) – 2
Aayakar Bhawan, Sector 3,
Vaishali, Ghaziabad,
Uttar Pradesh – 201010
(Tel): 0120-2770029
(Fax) 0120-2770452

Witness

1. ______________________________

2. ______________________________

Witness

1.

2.