



**ELECTRONICS CORPORATION OF INDIA LIMITED, HYDERABAD
INSTRUMENTS AND SECURITY SYSTEMS GROUP – PURCHASE**

ECIL:ISG:PUR:EOI:15-16/02:

Dated: 21th September, 2015

Expression of Interest (EOI)

The envelope of EOI shall super scribe “Expression of Interest” and must mention the REF NO. ECIL:ISG:PUR:EOI:15-16/02:

**Sr. DGM (MATERIALS)
INSTRUMENTS & SECURITY SYSTEMS GROUP
ECIL, HYDERABAD**



**ELECTRONICS CORPORATION OF INDIA LIMITED, HYDERABAD
SECURITY SYSTEMS AND PROJECTS DIVISION,
INSTRUMENTS AND SYSTEMS GROUP – PURCHASE**

LAST DATE: 15:10:2015 BY 15:00 hours

INVITATION FOR EXPRESSION OF INTEREST (EOI) FOR selection of OEM for customization, supply and integration of “*Video Analytics Integration Platform*” (VAIP) with *Video Content Analytics (VCA)* & *Video Surveillance System (VMS)*.

Electronics Corporation of India Limited (ECIL) invites Expression of Interest from reputed companies, having the product ‘**VAIP**’ and experience in supply and integration of IP based “*Video Surveillance System*” along with extensive “*Video Content Analytics*” solutions for an effective surveillance, for implementation of ***IP based Video Analytics Integration Platform (VAIP), Video Content Analytics (VCA) & Video Surveillance System (VMS)*** as part of **Integrated Security Solution** to one of its Govt. Customer at Delhi and surrounding regions. It is reiterated that only such companies that have successfully executed comprehensive surveillance system in major organizations/industries will be considered for pre-qualification.

Interested Firms who meet the pre-qualification criteria may furnish their Expression of Interest with all the necessary documents in a sealed cover along with the covering letter duly signed by an authorized signatory on or before 15-10-2015 by 15:00 hours at the following address:

TECHNICAL MANAGER (PURCHASE),

INSTRUMENT & SYSTEMS GROUP,

ECIL, Hyderabad - 500062

Telephone: 040-27182655

Fax: 040-27122540

Email: igmmgt@ecil.co.in

IP based Video Analytics Integration Platform (VAIP), Video Content Analytics (VCA) & Video Surveillance System (VMS)

EXPRESSION OF INTEREST (EOI)

FOR

Selection of OEM for customization, supply and integration of *Video Analytics Integration Platform (VAIP) with Video Content Analytics (VCA) & Video Surveillance System (VMS)*

**INSTRUMENTS AND SYSTEMS GROUP – PURCHASE
ELECTRONICS CORPORATION OF INDIA LIMITED
HYDERABAD**

CONTENTS

Page No.

1. EXPRESSION OF INTEREST.....	5
2. EXISTING CCTV SYSTEM AT CUSTOMER PREMISE.....	5
3. OBJECTIVE OF THIS EXPRESSION OF INTEREST (EOI).....	6
4. SCOPE OF WORK	6
5. FUNCTIONAL REQUIREMENT.....	9
6. TENTATIVE CALENDAR OF EVENTS	46
7. EXAMINATION OF THE “EOI DOCUMENTS”	46
8. VENUE and DEADLINE FOR SUBMISSION OF PROSPOSALS.....	46
9. ELIGIBILITY AND PREQUALIFICATION CRITERIA.....	47
10. RFP Bid Evaluation Methodology.....	54
11. DUE DILLIGENCE.....	55
12. VALIDITY OF THE EOI PROPOSAL.....	55
13. CLARIFICATION TO THE “EOI DOCUMENTS”	55
14. CONFIDENTIALITY.....	55
15. LANGUAGE OF EOI PROPOSAL.....	56
16. ANNEXUREs.....	57

1. Expression of Interest

Electronics Corporation of India Ltd, a leading Public Sector Company with Head Office at Hyderabad and Branch Offices at Metropolitan cities, is engaged in design, development, manufacture, supply and installation of state-of-the-art technology based solutions to core industrial, government and strategic sectors.

Security Systems and Projects Division of Electronics Corporation of India Limited (ECIL) invites expression of Interest from reputed companies, having “Video Analytics Integration Platform”(VAIP) as a product and experience in Supply and integration of IP based CCTV systems along with extensive content analytics solutions for an effective surveillance, to provide as a part of **Integrated Security Solution** to one of its Govt. Customer at Delhi and surrounding regions. The current EOI is floated to select suitable **OEM for customization, supply and integration of Video Analytics Integration Platform (VAIP) with Video Content Analytics (VCA) & Video Surveillance System (VMS)** for providing this solution. It is reiterated that only such companies having the product VAIP and that have successfully executed comprehensive surveillance system in major organizations/industries will be considered for pre-qualification. ECIL’s decision with regard to the short-listing of Firms through this EOI shall be final and ECIL reserves the right to reject any or all the EOIs without assigning any reason.

2. Existing CCTV system at customer premise:

In order to assist the security agencies in maintaining high level of security, a legacy CCTV system is functioning in the customer premise where this system is to be implemented. In this, a mix of analog and digital cameras is being used for capturing the video images from strategic locations.

The following security components which are otherwise not part of the CCTV system are also functioning in the premises so as to complement the security system.

- Fire Alarm
- Gunshot detector
- Glass Break detector
- Public Address system
- Panic Button
- Tetra system
- Access Control system, and
- Power fence

With the help of the integrated VAIP, VCA and VMS platform, it is being planned to have 24x7 continuous state of the art surveillance system, complimented with most advanced features, for the entire premises. The system would provide facilities for regular monitoring and analysis of the video feeds and to initiate automatic alerts upon security events as shall be predefined.

3. OBJECTIVE OF THIS EXPRESSION OF INTEREST (EOI)

The objective of this EOI is to solicit proposals from interested Firms for participation in a EOI process for the selection of **OEM for customization, supply and integration of Video Analytics Integration Platform (VAIP) with Video Content Analytics (VCA) & Video Surveillance System (VMS)** with fixed time warranty support and annual maintenance, if required, for one of our Govt. Customer at Delhi and surrounding regions.

4. SCOPE OF WORK

4.1 Introduction

The customer premise where this system has to be deployed is a high security area where the entry is restricted only to authorized persons. Visitors are allowed only after getting proper entry pass to a specific building/room. However, vehicles are generally not allowed inside the complex except in the case of VVIPs, Members, and senior level government officials. Any permitted item/material being taken inside the complex is thoroughly checked /scanned and proper entries made in the entry book. As the threat perceptions in the recent past has increased many fold and the existing CCTV system is not meeting the expectations of the security division, it is proposed to deploy a new state of the art and advanced **Video Analytics Integration Platform (VAIP) integrated with Best of the breed Video Content Analytics (VCA) & Video Surveillance System (VMS”)** to upgrade and complement the existing deployment.

It is planned to induct a high-performance CCTV system along with real-time video analytics software that transforms the standard surveillance system into an intelligent effective detection and alert system.

With the help of the proposed new system, it's planned to have 24x7 continuous surveillance of the entire customer premises. The system would provide facilities for regular monitoring and analysis of the video feeds and to initiate automatic alerts upon security events as shall be predefined. The objective of the system is to use the system to monitor all cameras at all times and when something unusual happens, to alert the security division to act on it and thus improve the effectiveness of the security system.

The system should capture, store and analyze digital video images to enable centralized monitoring, increase operational efficiency, reduce liability, minimize risks and secure people and property.

Authorized personnel should be able to rapidly zero in on images of specific locations, people and events, anytime, anywhere, without reviewing countless hours of video recordings. As part of event management after an operator confirms an event, a predefined response plan is dictated for optimal and efficient resolution.

4.2 Scope of Surveillance

The proposed system must assist the security authorities in better security management by providing state of the art surveillance solutions and help in automatically monitoring the videos of people, vehicles, objects and their associated behavior within the camera view.

The brief scope of activities as envisaged in this EOI is detailed below:

- 1) Supply, Customization, configuration, installation & commissioning of “Video Analytics Integration Platform” and integration with other systems as required.
- 2) The Solution should be robust, vendor-agnostic, open standard Video Analytics platform that taps into existing or new video surveillance cameras and provides real-time situational awareness for security and operations.
- 3) An integrated command and control application enables visualization of geo-coded alerts in a map interface.
- 4) The system should be able to take direct CCTV camera feeds across digital and analog formats as well as VMS system and create a centralized command and control center which allows plug and play integration of various Video Analytics.
- 5) Implementation in accordance with the acceptance criteria
- 6) Change management methodology and procedural adherence in change management
- 7) Training to be imparted to end users to be able to use the system for intended purposes
- 8) Adherence to approved project plan and project governance structure
- 9) The above mentioned solution should be able to address at a minimum functional use case / Scenarios and deploy, customized and adapt different algorithms from different OEM for Video analytics and have the facility to build different operational and predictive algorithms and simulations.
- 10) Apart from above requirements, the successful Firm must be prepared to work hand in hand with ECIL for joint development of the required application.
- 11) The Firm must share all technical details, without reservations whatsoever, that may be required for the joint development activity for enhancement or up-gradation of the product for ‘seamless integration’ with any other new applications that will be required to be developed for meeting the solution in entirety.

- 12) The Firm is expected to incorporate necessary changes in the supplied applications to achieve customization and must share the work flow for such enhancements.
- 13) The Firm must provide all required assistance in the form of APIs, SDKs, Work Flow/ flow charts for facilitating the understanding of the application.
- 14) The Firm is also expected to assess the training needs for the project and impart necessary training to ECIL engineers to familiarize them with the product as well as associated tools required for customization, development, integration and implementation. The training should also include necessary classroom presentation as well as hands on practical on the product.
- 15) Apart from the above training, imparted at the beginning of the project, 'need based' training session shall be organized by the Firm based on requirement arising during execution.
- 16) The Firm shall be able to provide Generic Solution comprising of but not limiting to the following modules/services:
 - a. Video Analytics Integration Platform (VAIP)
 - b. Video Analytics for each category listed below
 - c. Video Management System
 - d. Product Customization as per requirement
 - e. Training to the ECIL engineers to part in the customization/ integration/ updates activity
 - f. Special Development tools required if any

Any other component required for meeting functional requirements of the system.

4.3 Disaster Recovery System

In order to ensure high availability of the system and the historical video images for future analysis the Firm should draw a detailed plan of action for setting up a disaster recovery unit within the premises or elsewhere subject to not violating the rules and regulations on security. The disaster recovery system should strictly adhere to the best practices and standards.

The proposed solution should be tamper proof so as to mitigate any attempt to tamper with the security systems.

The system should offer analytical facilities like tracking of any event say, VIP special vehicle movement, accident happened if any inside the complex, crowd monitoring, fire, left baggage detection, face detection and recognition, automatic number plate detection and recognition, incident tracking etc.

5.0 FUNCTIONAL REQUIREMENT

5.1. VIDEO ANALYTICS INTEGRATION PLATFORM (VAIP)

5.1.1 ARCHITECTURE:

1. The (VAIP) shall use a flexible, open platform architecture built on accepted industry standards that facilitate integration with leading IT infrastructure.
2. The (VAIP) shall support running on COTS computer server, from a leading manufacturer (including IBM, Hewlett-Packard and Dell) with processors at minimum speed of 2.8 GHz from a leading manufacturer (including Intel or AMD); with a network-interface card with a minimum speed of 1GBPS. Hard-disk drive requirements should be identified during the system design preparations and be aligned accordingly.
3. The (VAIP) shall have a flexible, open architecture, and be able to migrate from a single site into a multisite system, e.g. components/servers comprised in the solution are deployable in a geographically disperse fashion.
4. The (VAIP) shall support a Workgroup Microsoft Windows Environment.
5. The (VAIP) shall have a flexible, open architecture built on accepted industry standards that supports an Active Directory Domain Environment.
6. The (VAIP) shall support single sign on (SSO).
7. The (VAIP) shall optionally be able to be installed in a Virtual Environment and be recognized by VMware as VMware Ready.
8. The (VAIP) shall offer redundancy solutions using the industry standard architecture like Marathon Ever Run or VMware ESXi platforms. The following possible solutions shall be supported:
 - The solution shall be redundant, using two separate servers, and achieve a fault tolerant, zero downtime environment and zero data loss, however may require manual or automatic start of the application on the secondary server.

- The solution shall provide a disaster recovery option, using a third separate server at a secondary location which would assume primary responsibility in the event of a catastrophic event at the primary location.
- 9. The (VAIP) shall possess an internal watchdog to detect and recover from the unlikely occurrence of a system lockup.
- 10. The (VAIP) Server component shall support latest version of Microsoft Windows
- 11. The (VAIP) Client component shall support Windows 8 (64 bit) operating systems for workstations.

5.1.2 (VAIP) INTEGRATIONS

1. The (VAIP) shall be an open architecture system allowing simple integration to external modules, sensors and systems, and allowing future scalability.
2. The VAIP application shall be able to integrate Alarm Videos from multiple Analytics application and display on user workstation on a single screen.
3. The VAIP application will get seamlessly plugged in from different vendors of Video Analytics.
4. The (VAIP) shall be vendor agnostic and have the ability to interface with any type of security, safety or other business systems including, and not limited:
 - a. CCTV Surveillance Systems
 - b. Fire, Smoke and Gunshot Detection Systems
 - c. Panic button systems
 - d. Access Control Systems and Badging systems
 - e. Perimeter and Intruder Detection Systems
 - f. Face recognition/detection systems
 - g. License plate recognition systems
 - h. GPS tracking systems
 - i. CAD Systems

The system integrator should spell out the necessary interfaces such as API, SDK, protocols required for integration of the above systems.

5.1.3 (VAIP) CLIENT COMPONENTS

1. The PC workstation used to operate the (VAIP) client application shall use equipment from a leading manufacturer.
2. System administration components
 - a. User management
 - b. Assets/Integrated system management
 - c. Maps management
 - d. Response planning
 - e. Audit trails
 - f. Dispatch planning
3. (VAIP) operator Client
 - a. Supervisor Dashboard
 - b. Assets Monitoring
 - c. Video Surveillance
 - d. Alarm management
 - e. Incident management
 - f. Search facility

5.1.4 (VAIP) FUNCTIONS

1. User Management
 - a. The system shall support native authentication (e.g. against its own servers and stored credentials).
 - b. The system shall support authentication against Active Directory.
 - c. The system shall have the ability to order users in hierarchal groups structure.
 - d. The system shall have the ability of disabling\enabling existing user account without deleting it.

- e. The system shall allow capturing user's data (include name, e-mail and phone number) as part of the user account creation.
 - f. The system shall provide for the definitions of roles where each role has a set of configurable privileges.
 - g. The system should group privileges based on modules and functionality areas and allow multi selection of all privileges in a group.
 - h. The system shall have the ability to assign a role to a user and define the devices scope that this role applies to.
 - i. The system shall have the ability to effectively assign multiple sets of privileges on multiple sets of resources/devices to a single user.
2. Integrated systems management (assets)
- a. The system shall allow managing integrations servers from a central administration application.
 - b. The system shall support multiple integrations servers working with the same application and database servers.
 - c. The system shall allow adding new system adaptors to integration server from a central administration application.
 - d. The system shall allow configuring the system adaptor connection information (IP, user, password) from a central administration application.
 - e. The system shall allow discovering the devices of the integrated system and allow the administrator to define/select which devices should be monitored by the system.
 - f. The system shall allow viewing the discovered device in a list and enable sorting of that list based on device type, name, monitoring state.
 - g. The system shall allow selective monitoring of subset of all available devices of a specific integrated system.
 - h. The system shall allow assigning a display name and a description for the integrated device.
 - i. The system shall allow ordering the monitored devices in a multi-level tree structure that represents the organizations operation hierarchy.

- j. The system shall show icon, next to each device entry, that represents the device type.
- k. The system shall allow filtering the monitored devices tree by device type.
- l. The system shall allow searching the monitored devices tree by device name.
- m. The system shall allow creating relationships between devices of same or different systems. These relationships shall be used for automation, accessibility, etc.
- n. The system shall allow creating relationships between a device and a PTZ camera and specific preset.
- o. The system shall monitor and ensure that enabled system adaptors are up and running.

3. Maps management

- a. The system shall allow definition of multiple maps.
- b. The system shall allow ordering the maps in a hierarchal tree structure.
- c. The system shall allow adding multiple layers to a map.
- d. The system shall provide the administrator with a feature-rich map control and browsing capabilities.
- e. The system shall allow adding layers from service sources including Open Street Map, ArcGIS online and ArcGIS servers.
- f. The system shall allow adding layers from registered file formats as well as unregistered file formats.
- g. The system shall allow having online service layers and local files layers on the same map.
- h. The system shall allow ordering the layers in a hierarchal tree structure.
- i. The system shall allow adding monitored devices layers and place devices on them.
- j. The system shall enable searching for a device by name or type in order to select if for placing.
- k. The system shall allow interacting with the device (play video for cameras, close relays) from the map management module.
- l. The system shall allow removing a device from a specific layer.

- m. The system shall allow editing device's GIS location by locating it on the map or by inputting its exact GIS coordinates.
 - n. The system shall allow viewing the layer that the device is included in from the device icon on the map.
 - o. The system shall save the map context (extent, layers selection) when browsing between maps.
 - p. The system shall allow defining zoom-in and zoom-out levels per layer. Such customization will allow showing layers of different details level at the right context.
 - q. The system shall allow defining cameras and devices coverage area. Coverage area should include coverage area range, angle and orientation.
 - r. The system shall display device coverage area as a semitransparent polygon on the map.
 - s. The system shall allow showing\hiding the coverage area for a single or all devices.
 - t. The system shall allow adding point of interest markers that can also include links to other maps and will be used as on-map hyperlinks.
 - u. The system shall enable administrator to grant privileges to manage maps and\or place devices.
4. Incident response planning
- a. The system shall allow management (Add, delete, modify and rename) of incident types.
 - b. The system shall support management of response procedures.
 - c. The system shall support adding to-do tasks in the response procedures.
 - d. The system shall support adding decision tasks with multiple options in the response procedures.
 - e. The system shall support adding manually initiated device command tasks in the response procedures. Device command tasks should include sending camera to preset, control doors, dispatch, etc.
 - f. The system shall allow selecting which device to apply the command to. Automatic device selection (based on event that triggered the incident) or manual selection should be supported.

- g. The system shall support adding automatically initiated system command tasks in the response procedures. System command tasks should include sending e-mail (optionally).
- h. The system shall support automatic initiation of device and system commands upon incident creation.
- i. The system shall enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.
- j. The system shall allow configuring and executing incident triggering rules.
- k. The system shall allow setting up multiple triggering rules per incident type.
- l. The system shall allow enabling\disabling rules and this change should take effect on the fly.
- m. Incident triggering rules should include conditions referring to the following data event details: event type, event sub type, event source device, event description.
- n. The system shall enable setting the severity and the response procedure that will be associated with the automatically triggered incident.
- o. The system shall allow adding dispatch commands as part of the response procedures.

5. Audit trails

- a. The system shall retain/store all user activity audit records for a period of 2 years.
- b. The system shall provide an application for searching these records.
- c. The system shall provide audit record search capability based on time, user name, user full name, action description and IP address.
- d. The system shall display audit records search results in a tabular structure that supports sorting, grouping and searching within results.
- e. The system shall allow exporting the audit search results into a tabular file format (e.g. XML).

6. Dispatch Incident

- a. The system shall allow mapping incident/mission dispatch.
- b. The system shall allow different dispatch missions based on incident severity.

- c. The system shall allow automatic system initiated and/or manual operator incident dispatch request.
- d. The system shall report upon successful dispatch request.
- e. The system shall allow request of mission abort.
- f. The system shall update the incident record on all dispatch system reports including dispatch ongoing status and responders allocation and ongoing handling reports.
- g. The system shall support responders initiated alarms (e.g. panic alarm).
- h. The system shall allow manual dispatch of responders to an active incident.
- i. The system shall automatically close the dispatch mission upon closure from all responders and fulfillment of the dispatch rule.
- j. The system shall validate completion of an active dispatch upon incident closure.

7. Supervisor Dashboard

- a. The system shall provide supervisors with a KPI driven dashboard that measures the performance of the control room.
- b. The dashboard should include performance visualization related to alarm handling and follow alarm response time KPI, number of active alarms.
- c. The dashboard should include performance visualization related to incident handling and follow average incident response time KPI, active incident resolution time KPI.
- d. The dashboard should include counters and graphs displaying number of alarms and incidents and also by severity and by type distribution graphs.
- e. The dashboard should include a map for laying out the information geographically. User should be able to set the map and its extent.
- f. The dashboard should allow drilling down to the relevant module (alarms or incidents) from a specific graph /gauge /Time.
- g. The system shall allow administrators and/or Supervisor to setup the customer specific KPI numbers.
- h. The system shall allow the user to order the dashboard components.

8. Assets monitoring

- a. The system should present the operator with a logical tree that contains devices from different types.
- b. The system should enforce that each operator sees only the defined device scope.
- c. The system shall allow searching the device tree by device name or device type.

- d. The system shall indicate the device type by an icon.
- e. The system shall allow sending commands to a device from its tree entry or its map icon. Sending commands privilege should be configurable as part of the user role.
- f. The system should display the related devices for the selected device.
- g. The system should display the devices on maps as icons that correspond to the device type.
- h. The system should display a pop-up for a device with its details.
- i. The system should allow zooming the map to a device location from the device entry in the tree.
- j. The system shall update the maps of all logged in operators with location change that is received from GPS tracked devices.
- k. The system shall display an icon for each device that is placed on map.
- l. The assets map should allow pan, zoom, and rotation via standard mouse operations (e.g. wheel for zoom-in\out) and on map control.
- m. The system shall enable to operator to show\hide background or devices layers.
- n. The system shall cluster devices whose icons overlap so that the map is not cluttered when zooming out.
- o. The system shall allow operator to set the device icons clustering sensitivity.
- p. The system shall allow operators to show\hide devices coverage area.
- q. The system shall allow operators to request to see live video from cameras whose coverage area is covering a point on the map selected by the operator.
- r. The system shall support playing live video of cameras or for devices associated camera.
- s. The system shall support geo-association; pinning an area of interest on the Map and as a result, automatically showing all the devices which have coverage on the pinned area and for the relevant camera devices, play live video.

9. Alarm management

- a. The system shall display all alarms in a unified grid.
- b. The system shall support sorting and filtering of the alarms grid based on every displayed column.
- c. The system shall support text based searching in the alarms grid.

- d. The system shall visually notify operators upon receiving new alarms in a non-blocking manner. The visual notifications can be turned on\off per operator's preference.
- e. The system shall allow clearing alarms. Cleared alarm should be visually different from active alarms.
- f. The system should update the alarm record on all operators workstations when an operator clears an alarm.
- g. The system should log and display the time and the user name of the operator that cleared the alarm.
- h. The system should display the alarm details upon alarm selection. Details should include source device and its related devices, alarm meta data, alarm attached images.
- i. The system shall allow zooming in on the alarm location.
- j. The system shall allow viewing recorded video from the time of the alarm. System should deduce the relevant camera based on the alarmed device and its related cameras.
- k. The system shall enable opening all alarm related video (live and recorded) in the video workspace.
- l. The system should display the alarm record, its details, its location and related video in a single screen.

10. Incident management

- 1) The system shall display all active incidents in a unified list.
- 2) The system shall support sorting and filtering of the incident list based on every displayed column.
- 3) The system shall visually notify operators upon receiving new incidents in a non-blocking manner. The visual notifications can be turned on\off per operator's preference.
- 4) The system shall update the incident record on all operators workstation for any activity done by the operator on the incident ensuring consistent common operational picture.
- 5) The system shall allow creation of new incident with/without geographical context.
- 6) The system shall allow the user to set the type, severity, description, time, response procedure of the manually created incident.

- 7) The system shall capture as much information from the new incident creation context and populate it to the incident (time, description, location).
- 8) The system shall allow the user that creates incident to auto assign it to him\her.
- 9) The system shall allow taking ownership of unhandled incidents. This action should be managed by a dedicated privilege.
- 10) The system should log and display the time and the user name of the operator that accepted the incident.
- 11) The system shall allow editing the incident severity, timestamp and description. Upon editing incident severity, user that is viewing this incident should get visual notification that the severity was changed.
- 12) The system shall allow setting and changing incident location.
- 13) The system shall allow the owning user to close the incident.
- 14) The system shall suggest the user to add incident summary upon incident closure.
- 15) The system shall allow exporting an incident summary report in pdf format, saving and viewing it. The incident summary report should include the incident details, attachments and their image preview, chronological activity timeline with the main incident lifecycle information.
- 16) The system should display the incident details upon incident selection. Details should include relevant response plan, logged activities performed on the incident, attachments (including source alarm) and incident source device and its related devices.
- 17) The system shall allow zooming in on the incident map location. The selected incident map icon should be highlighted.
- 18) The system shall include full map capabilities in the context of the incident where user can select map, layers, interact with on-map items, etc.
- 19) The system shall allow viewing recorded video from the time of the incident. The system should deduce the relevant camera based on the alarmed device and its related cameras.
- 20) The system shall enable opening all incident related video (live and recorded) in the video workspace. Recorded and live video from the same camera should be displayed side by side.
- 21) The system should display the incident record, its details, its location and related video in a single screen.
- 22) The system shall allow attaching map & video snapshots to the incident.

- 23) The system shall allow attaching video tags to the incident.
- 24) The system shall allow viewing incident attachments including maps and video snapshot in its default viewer. In case of video tags, the system shall allow viewing the tagged video in the video workspace.
- 25) The system shall allow attaching\removing events/alarms to an incident.
- 26) The system shall allow viewing incident attached alarms details. Details should include source device and its related devices, alarm meta data, alarm attached images.
- 27) The system shall allow zooming in on the attached alarms location and playback of alarm related video.
- 28) The system shall allow adding comments to the incident. Each comment shall be logged with the operator user name and the comments time stamp.
- 29) The system shall allow operator to execute the incident response plan.
- 30) The system shall display for each of the response plan tasks its description.
- 31) The system shall log all response plan tasks executed by the operator.
- 32) The system shall present response plan execution overall progress.
- 33) In case of decision point tasks, the system shall allow the operator to review the different optional routes before taking the decision.
- 34) In case of command tasks, the system shall allow operator to continue working while command is being executed.
- 35) The system shall support multitasking between incidents. When browsing between incidents, the incident form state (map, video, selections) should be persisted so the user will continue operation from same place.
- 36) The system shall allocate a video workspace per incident so videos not related to that specific incident tasks (e.g. routine monitoring, alarm assessment) will not be mixed.
- 37) The system shall persist the video workspace of the incident when multitasking between incidents so user will not lose the video context when browsing between incidents.
- 38) The system shall support incident response collaboration between multiple operators. Multiple operators should be able to mark tasks as done, add comments, and add attachments to the incident. Every change in the incident should be populated across all workstations.

- 39) The system shall enforce that operators are getting visibility for incidents based on their visibility to the device that triggered the incident.
- 40) The system shall enable visibility for incidents that are not associated with a device based on the defined organizational tree hierarchy. Colleague users in the same group and users higher in the hierarchy of the incident creating user should gain visibility to that manually created incident.

11. Search Facility

- a. The system shall provide search capabilities on all event, alarms and incident records.
- b. The system shall provide Incident record search capability based on Incident ID, type, description, time and severity.
- c. The system shall display incident records search results in a tabular structure that supports sorting, searching within results.
- d. The system shall allow viewing selected incidents details.
- e. The system shall allow exporting the Incident /event search results into a tabular file format (e.g. CSV).
- f. The system shall provide events record search capability based on event type, sub type, time and severity and source devices.
- g. Based on the event type, the system shall provide type specific custom fields as search parameters.
- h. The system shall display events records search results in a tabular structure that supports sorting, searching within results.
- i. The system shall allow creating new incidents from the event record.
- j. The system shall allow attaching of an event record to an active incident.

5.2. Functional use case /Scenarios in brief

- i. **Content (Video) Analytics:** The user console of the solution should have a feature of displaying all the various forms of alerts along with the video of the incident causing the alert to the users. It should allow the user to choose from a list of activity options. The various kinds of incidents and the capabilities required for the user to act upon an alert are listed below. In addition the user should be allowed to centrally summon any of the video feeds as required and act on them in similar fashion to the alerts.
- ii. **Identification of vehicles and persons of interest**
 - a. **Vehicle Number Plate Detection and Recognition:**

- i. Suitable cameras to be identified and installed in parking areas for number plate recognition which would work in varying light conditions, varying vehicle speeds and varying height at which the License plates are fixed with vehicle. The solution provider can suggest the type camera suitable for the best recognition of ANPR in all the lighting conditions and considering the Head Lights of the vehicle during the night.
- ii. The solution should monitor and recognize number plates on camera and should compare them with watch-lists to alert users on positive identification of any vehicle against such watch-list.
- iii. Officials/Members use Vehicles of different types, makes and models. In these vehicles there is no fixed standard adopted in the license plate and the plates are fixed at different heights and written in different fonts and languages. In some cases bumpers are placed at height which practically blocks clear view of the number plates. Solution shall be catering to all the above the scenarios to detect and recognize number plates.

b. Face Detection and Recognition:

- i. Suitable cameras to be identified and installed for detection and capture of faces at the most appropriate angle to be processed by the facial recognition system. Reconstruction of front view of a face where such a view is not captured by the camera would be required.
- ii. Captured faces are to be compared with a watch-list of images that will be provided at the time of development and a match should trigger an alert with all relevant information leading to the match including live image, watch-list image and details from the watch-list.
- iii. Solution Provider is required to provide a comparison of commonly used algorithms and software available in the market with success rate in similar installations and provide information on adoption elsewhere.

- iii. **Abnormal activity detection and alerts with appropriate categorization:** Provided below is a list of abnormal activities envisaged for video analytics and the requirements pertaining to the same. The Solution Provider is required to propose any additional abnormal events that can be considered for triggers.

- a. **Crowd Detection:** The accurate count of people in identified areas within the premises is to be monitored and alerts are to be triggered when the count of people exceeds threshold levels. The threshold levels might vary for the same designated area depending on factors like working day/holiday.
- b. **Counter Flow Detection:** On identified routes for vehicle movement, any vehicles traversing in the opposite direction should be accurately identified and alerts triggered off to the concerned authorities along with a category of aberrant vehicle

as a two-wheeler, car, truck etc. The system should not generate false alarms against birds, shadow, vegetation branch oscillation (due to wind) etc.

- c. **Illegal Parking:** Vehicles not authorized for parking and vehicles parked outside the designated areas should be identified accurately and alerts triggered off to concerned authorities. Illegal parking would be required to be distinguished from incidental vehicle stoppages to drop and pick-up passengers.
- d. **Intrusion Detection:** Cameras set up along the perimeter should be monitored by the solution to identify perimeter breaches by individuals or objects and requisite alarms are to be raised. The following should be adequately addressed:
 - i. Algorithms are required to be sophisticated enough to ignore animals and movement of foliage and puddles of water etc. and the solution should allow incorporation of better algorithms when available.
 - ii. Distance to, the size and speed of the object or person of interest are to be automatically calculated and alarms to be triggered in case of either parameter cross the threshold levels prescribed.
- e. **Left/Unclaimed Baggage Detection:** The solution should accurately identify unclaimed/left baggage and objects and trigger alerts for baggage and objects left unattended beyond a threshold of time that would be decided.
- f. **Compound alerts:** The solution should be able to build customized rules with customized levels of severity and protocols. For instance in case of an vehicle watch-list match and an unclaimed foreign object happening within minutes of each other the level of alert should be of higher severity than the two events happening independently and might follow a different automated escalation matrix.

iv. Tracking capabilities

- a. **Vehicle Tracking and Management:** The solution should be able to track vehicles across multiple cameras from entry to exit. Post triggering of alert in cases of abnormal activity or watch-list match, the solution should identify and transmit the location of the vehicle on a map. The solution should allow for any given vehicle to be tracked back across recordings from multiple cameras.
- b. **Persons of interest tracking:** The solution should be able to track individuals across multiple cameras from the point of entry to point of exit. Post triggering of an alert the solution should be able to identify and transmit the location of the individual on a map. In case of alerts due to reasons other than the watch-list, the solution should also be able to track the person across recordings from multiple cameras.

v. Other key features

- a. **User-friendly interfaces:** The solution should be intuitive to use and user-friendly with minimal learning time to understand the comprehensive feature list of the solution.

- b. **Real-time alerts:** The solution should trigger all alerts on a real-time basis as soon as the incident leading to the trigger occurs.
 - c. **Camera malfunction alerts:** Any instance of a camera malfunction or loss of data feed is to be highlighted to the maintenance team immediately.
 - d. **Handling camera malfunction:** The solution should skip a malfunctioning camera to show the image from the next camera with near-zero waiting time
 - e. **Stitching of images:** The solution should allow multiple images from overlapping cameras to be stitched to create larger views of the premises
 - f. **Visualization of camera feeds:** The solution should enable automatic viewing of live feeds from various cameras both sequentially as well as simultaneously over multiple screens or split screens.

- vi. **Analytical Reports:** The solution should enable the user to configure and generate various reports from archived information
 - a. **Vehicle movement report:** The solution should allow the user to generate a report based on vehicle movement patterns of interest such as abnormal halts, halt duration etc.
 - b. **Parking utilization:** The user should be able to generate a periodical report on the utilization of parking space that can aid in better planned parking management.
 - c. **Illegal parking report:** The user should be able to generate a periodical report on incidents of illegal parking at regular intervals that would analyze the trends of illegal parking over time etc.
 - d. **Peak hour crowd analysis report:** The user should be able to generate a periodic report on the number of people assembling at a specified locations at various times of day.
 - e. **Unclaimed baggage report:** A user should be able to generate a periodic report on the incidents of unclaimed baggage identified.
 - f. **False alarm analysis:** The user should be able to generate a period report on false alarms thus aiding a root cause analysis for the false alarms and help in improving the solution performance.
 - g. **Uptime analysis of CCTV components:** The user should be able to generate a periodic report on the uptime of individual CCTV components
 - h. **Audit trail and log analysis:** The solution should be enable generation of periodic reports on audit trails. Audit trails should comprehensively capture all details of individual transactions including user id, time stamps, action performed. Access to the audit trails is to be restricted to the super system administrator who should be able to generate reports on various kinds of transactions such as unauthorized login attempts etc.
 - i. **Stored device configuration:** The system is required to generate reports of stored device configuration. The control software is required to provide alarm and alarm

log. The log shall be able to be archived, printed and displayed using a device filter, a device group filter and/or a time window.

- vii. **Leveraging other data sources:** The solution should be capable to accept data sources other than video feeds such as inputs via appropriate interface etc. to identify correlations with identified alerts to build predictive capabilities.
- viii. **Performance metrics:** The number of false alarms should not be more than 10% of all alerts triggered.

5.3 Video Analytics Specifications:

- i. **Vehicle Tracking and Management**

If there is any violation of norms by any of the vehicle, the system should generate alarm immediately so that action can be initiated on a near real time basis. In any case alarm should be generated within 5 seconds of the event, that is the violation happened and also that the number of false alarms should not exceed more than 10% of the total alarms.

- ii. **Incident tracking:**

The system should offer facility to track vehicular movement of VVIPs happened in the PH complex area in a real time basis and also offer facility to play back later on. For example, the VIP movement which might take place in dedicated routes may be tracked in a real time basis. The operator or any authorized official should be in a position to track the movement of the vehicles from the designated entry point up to the exit gate of the complex. As the vehicles generally moves at a high speed, the system should be capable of switching cameras at faster pace. The changeover time for cameras should be bare minimum. The entire tracking module should be an automated process and should not involve any manual intervention. In case of any camera malfunctioning due to any unforeseen reason the system should automatically identify the issue and move on the next camera with near zero waiting time. An acceptable threshold level needs to be worked out for camera switching time, skipping of malfunctioning camera, etc. in case of failure of any camera ALERTS should be sent to the maintenance group and to the controller in a near real time basis along with the kind of alarm. Stitching of multiple camera views to create virtual cameras with much larger views.

The system should offer two types of incident tracking, viz. (i) a quick launch system by which all the cameras are to be displayed on the same display unit sequentially without any

human intervention, (ii) display the tracking on multiple screens/split-screens of the same user so that even if any of the camera mal-functions the others does not get affect.

iii. Counter Flow Detection

There are certain routes identified for VIP movements. For security reason in those designated routes vehicles are allowed to traverse in a unidirectional mode. The system should detect any vehicle traversing in the opposite direction, generate alarm, and broadcast to all the concerned officials for remedial action. Flying birds or any other small objects should not be detected as counter flow movement. Except the moving vehicles all other objects may be ignored by analyzing/calculating the size of the object and its duration of presence in the camera coverage area. If any bird crisscross along the counter flow route that also should be ignored.

iv. Vehicle Number Plate detection and Recognition

There are two phases in the vehicle number plate detection and recognition system. First, the system should detect the license number of the vehicle entering the PH complex. A perfect process should be evolved so as to detect the right number at the correct angle. Once the license number is detected it needs to be matched with the entries in the database. In case the detected number matches with any of the stored entries in the database an alert should be generated on a near real time basis. The database of suspected and blacklisted vehicle registration numbers would be made available at the time of development. Suitable cameras should be installed in the general parking areas so as to capture the Vehicle License Number Plates so that the vehicles can be easily tracked from its entry into PHC till it leaves the complex.

v. Illegal Parking

Authorized vehicles are allowed to park at designated places only. For different level of officials and VVIPs/MPs separate designated parking areas are assigned. If any vehicle is parked in any other location the system should identify that vehicle, using the help of Camera feed analytics and License Plate Reader, and immediately generate alarms. If a vehicle travels for some time/distance and then halt in the no parking area so as to drop a VVIP/VIP/MPs/officials and then moves out of that area then it should not be treated as illegal parking. In case the halt time exceeds a defined level say, two minutes then raise an alarm.

Any object kept at the parking area should not be detected as illegal parking. If more than one vehicle enters (at different time period) and halts at the Illegal Parking area at a given range of time period then the vehicle which halted for more than the allowed time limit need to be identified for its evacuation. This could be possible with the help of LPR and

tracking the vehicle from the time it enters into the PH Complex and up to the present halting point.

vi. Intrusion Detection

In the perimeter area cameras should be fixed so as to capture any object or human intruding into the secured areas. In the present setup the system generates large numbers of false alarms due to foliage, tree branch oscillation, shadow, water patches, headlights of vehicles passing by during night, and birds/monkey movement etc.

In order to have an efficient Intrusion Detection system it should have better filtering algorithms built in it and should also have provision to add new and improvised filtering algorithms. Before generating alarms the system should first determine the distance (focal length) between the object and camera, using distance calculate the actual size of the object. If the size and distance are less than threshold levels, ignore it, else generate alarm. If an object is thrown or a living thing jumps from the outer side of the wall at a much higher position than the height of the wall (say, jumps at a height of one meter above the wall height) the camera should capture the image and content analytics performed on that image. Based on the analysis it should decide whether the object crossing the periphery is a threat or not.

In the present setup cameras are positioned at the wall level and capture the images only at a horizontal level. In the proposed approach cameras should be positioned at much higher level than the height of the wall so that it will have a wider coverage area.

vii. Crowd Detection

There are certain areas within the PH complex where the number of people assembles at any given point of time needs to be monitored. For each of the identified area the maximum number of people allowed is fixed and the number may vary from time to time and area to area. The camera should capture the numbers, do the analysis, and generate alarm, if the number exceeds the acceptable level. In order to capture the exact number of assembled people in the said area cameras should be positioned at the right place so that shadows or any other objects are not part of the final count. Shadows of human being assembled in the said area should not be counted as crowd. There must be a provision to specify the maximum numbers of people allowed to assemble at any given point of time in the identified areas.

viii. Face Detection and Recognition

There are two phases in the face detection and recognition system. First, the system should detect the face of the person visiting the premises. A perfect process should be evolved so as to detect the face at the correct angle. The system may also detect the person's face front view or side view at varied angles. Once a face is detected it needs to be matched with

the existing database. In case the detected face matches with any of the stored entries in the database an alert should be generated on a near real time basis. The database of suspected and blacklisted people's photographs would be made available at the time of development. This module requires a detailed analysis of the algorithms/software available in the market, its success rate in other CCTV applications elsewhere, and exact requirement in the current scenario in the premises.

ix. Left/Unclaimed Babbage Detection

Any unclaimed object lying for more than a specific time should be identified and alarm generated. Shadows, water patches, distinct colored 2-dimensional objects should not be detected as unclaimed objects. At most care should be given before deciding on the object. Improvised 3-dimensional models could be used for identifying the objects so that minimal numbers of alarms are generated in the process. The positioning of camera also should be at a decent height so that shadows won't be counted as objects.

5.4 Video Management System (VMS)

5.4.1 VIDEO MANAGEMENT SOFTWARE (VMS) ARCHITECTURE

The VMS shall have a flexible, open video, over IP architecture built on accepted industry standards that facilitate integration with IT infrastructures. The VMS should have the below mentioned features:

1. The VMS shall have a flexible, open architecture built on accepted industry standards that supports a Workgroup Microsoft Windows Environment, DNS/DHCP; Windows based authentication and an Active Directory Domain Environment.
2. The VMS shall be able to be installed in a Virtual Environment and be recognized by VMware as VMware Ready. A certificate of collaboration with VMware is to be attached.
3. The recorders shall use standard Commercial Off-The-Shelf (COTS) server technology and storage systems.
4. The VMS shall facilitate Firewalls Traversing for the Review application, Web Review, and Client Software Development Kit (SDK) connections.
5. The VMS shall facilitate video resolution transcoding, in order to stream video in a low bandwidth environment to the Review, Web Review, and Client SDK applications.
6. The VMS shall have flexible throttling technology that facilitates video streaming support for both software and hardware VPN, as well as for Review, Web Review and Client SDK remote applications' connections.

7. The VMS shall support Multiple NIC for Servers from different networks, which allows Client SDK applications to reach the Video LAN.

5.4.2 Redundancy of the System:

1. The VMS shall offer redundancy solutions like Marathon EverRun or VMware, ESXi platforms or equivalent platforms by supporting the following:
 - a) The solution shall be redundant, using two separate servers, and achieve a fault tolerant, zero downtime environments.
 - b) The solution shall provide a disaster recovery option, using a third separate server at a secondary location which would assume primary responsibility in the event of a catastrophic event at the primary location. The solution shall be redundant, using two separate servers, and achieve a high availability, minimal downtime environment. This design should not result in any data loss, however may require manual or automatic start of the application on the secondary server.
2. The VMS shall support multicast capability to allow client applications to receive live streams from multicast groups through Switch/router instead of Recorder to provide live streaming continuously even when Recorders or the Server become unavailable.
3. The recorder shall offer a redundancy solution using a Dual Recording feature, with distributed architecture that allows each subsystem to operate independently, without affecting video recording or live viewing.
4. The VMS shall possess an internal watchdog to detect and recover from the unlikely occurrence of a system lockup.
5. The VMS shall provide support for IP (network) cameras from multiple third-party manufacturers using various codecs, including H.264, MPEG-4, and MJPEG.
6. The VMS shall be able to support video motion detection. This operation can be executed by the edge device, the IP Camera or the server. Enabling motion detection shall be performed either:
 - i. On a continuous basis
 - ii. As scheduled for particular times, dates, days, months, etc.
 - iii. For defined areas of interest, defined using an easy-to-use user interface and simple editing tools
 - iv. At a defined sensitivity level
7. The VMS Server component shall support software designed for the Microsoft Windows latest server platforms (64 bit).
8. The VMS Client component shall support Microsoft Windows 8 or higher (64 bit) operating systems for workstations.
9. The VMS shall support both single and multi-site deployments.
 - i. For multisite deployments, a multisite directory shall store information for all sites. A copy of the multisite directory shall also reside on each site in the

multisite configuration, avoiding any single point of failure. In the event of a multisite directory disconnection, each user shall still be able to execute multisite functionality.

- ii. The VMS multisite system shall have the ability to simultaneously view multiple cameras (live or recorded), alarms, bookmarks, and investigations, from any site, with a single sign-on for authorized users.
- iii. Sites can cross connect as required at any time by a simple configuration with a passkey.
- iv. The VMS shall have a flexible, open architecture that allows alarm event and response creation, whether for a single site or multisite, through an event and response manager that supports schedules and custom scripts.

5.4.3 VMS INTERFACES

- 1. The VMS shall support third-party IP cameras from at least 10 reputed manufacturers, using auto discovery functionality.
- 2. The VMS shall be Conformant to the ONVIF profile S standard for Network Video Client (NVC). The VMS shall be listed on the ONVIF.org web site list of conformant NVC products
- 3. The VMS shall support H.264, MPEG-4, and MJPEG compression from edge devices and IP cameras on a camera-by-camera basis.
- 4. The VMS shall support an unlimited number of dry-contact inputs and an unlimited number of relays outputs.
- 5. The VMS shall support any third party Keyboard/joystick
- 6. The Recorders shall use standard Ethernet connection for video input via TCP/UDP/IP.
- 7. The VMS shall support either or both unicast or multicast over the enabled network.
- 8. The VMS shall generate alerts on disabled camera inputs based on loss of communication signal or device being off-line.
- 9. The VMS shall support multiple frame rates ranging from 1 to 25 fps
- 10. The VMS shall support the following video resolutions:
 - a. QCIF
 - b. CIF
 - c. 2CIF
 - d. VGA
 - e. 4CIF
 - f. HD720
 - g. HD1080
 - h. 2MP

- i. 3MP
- j. 5MP
- k. 10MP

5.4.4 VMS VIDEO DEVICE SUPPORT

1. The VMS shall support the following Intelligent Edge Device and IP cameras:
 - a) Single input encoders and decoders
 - b) Multiple input encoders
2. The VMS shall be ONVIF profile S compliant
3. The VMS shall support third-party IP cameras from at least 10 different manufacturers, using auto discovery functionality. Cameras supported should be inclusive of, but not limited to the following brands:
 - a) Arecont
 - b) Axis
 - c) Bosch
 - d) DVTel
 - e) Mobotix
 - f) Panasonic
 - g) Pelco
 - h) Samsung
 - i) Sony
 - j) Verint
 - k) Canon
 - l) LG
 - m) XTS
 - n) Scallop Imaging

5.4.5 VMS SERVER COMPONENTS

a) Master Server

1. The VMS Master Server shall maintain cohesive operations of all of the components in the video management system, including the VMS database.

2. The VMS Master Server shall support up to 2,000 cameras and/or encoder channels on a single recommended Server. Multiple servers may be used to support a larger number of cameras.
3. A single Master Server shall support up to 100 servers used as Recorders, Enterprise Storage Manager (ESM) servers, Media Gateways, or Surveillance Analytics servers.
4. Each individual Master Server shall support a maximum of 80 Review application workstations simultaneously. To achieve a system configuration greater than 80 Review application workstations multiple servers may be used. In a multi-server configuration the maximum number of Review workstations is unlimited.
5. The Master Server shall be hosted on a COTS computer server with a hard-disk drive at minimum storage capacity of 250GB; and a network-interface card with a minimum speed of 10 GBPS.

b) Recorder

1. The VMS Recorders shall be certified with optional storage solutions.
2. The VMS Recorders shall be certified to record in a VMware environment.
3. The VMS Recorder Server shall have the ability to run Master Server functions, including the Recording and Review applications simultaneously.
4. The Recorder shall run autonomously, and continue to record once configuration is received.
5. The Recorder shall offer a fail-over solution, either to another recorder or group of recorders, dynamically, and without any user intervention.
6. The VMS Recorder Server shall have the ability to simultaneously record multiple streams.
7. The VMS Recorders shall store video on COTS computer server, from a leading manufacturer (including IBM, Hewlett-Packard and Dell); with processors at minimum speed of 2.8 GHz from a leading manufacturer (including Intel or AMD); with a network-interface card with a minimum speed of 1GBPS. Hard-disk drive requirements should be identified during the system design preparations and be aligned accordingly.
8. The recorders shall be capable of supporting the attachment of external storage devices via SAN, NAS, SAS, iSCSI or Fiber Channel.

c) Enterprise Storage Manager (ESM)

1. The ESM shall accept video files from multiple recorders for redundant, off-site, or long-term storage.
2. The ESM shall allow for the support of long-term video storage, using hard drives as the storage medium. It shall support virtually any central disk storage device, including disk arrays with iSCSI connectivity, Storage Area Network (SAN) and Network-Attached Storage (NAS) devices.
3. The ESM shall be capable of offering long-term video storage using COTS equipment with processors such as Intel or AMD.

d) Media Gateway Server

1. The Media Gateway Server shall transcode received video from IP cameras or edge devices at a certain resolution, and then convert, and send a lower resolution video through a bandwidth limited WAN link.
2. The Media Gateway shall support bandwidth as low as 56 kb/s for remote viewing through Web Review, and 256 kb/s through Review.
3. The Media Gateway shall support Review application User Priorities, in case multiple remote requests for video by Review users exceed the bandwidth of the WAN/LAN link.
4. The Media Gateway shall be capable of running all video transcoding, pass through, and WAN transport services, using COTS equipment with processors such as Intel or AMD.

5.4.6 VMS CLIENT COMPONENTS

a) Control Center Client Application

1. The VMS shall provide a Control Center client application, designed for system administrators to configure cameras, recorders, schedules, users, and system functions.
2. The PC workstation used to operate the Control Center application shall use COTS equipment with processors such as Intel or AMD.

b) Review Client Application

1. The VMS shall provide a Review client application, designed for operators to operate and view live/recorded video.
2. The PC workstation used to operate the Review application shall use equipment from a processors at minimum speed of 2.8 GHz from a leading manufacturer (including Intel or AMD); with a network-interface card with a minimum speed of 1GBPS; with a hard-disk drive with a minimum capacity of 250GB; with a high-end video card with 1GB RAM, 1024 x 768 screen resolution and highest 32-bit color quality.

c) Web Review Client Application

1. The VMS shall provide an ultra-thin, secured Web Review client application, designed for viewing by corporate personnel or other investigators.
2. The Web Review download with ActiveX shall be less than 3.5MB.
3. The PC workstation used to operate the Web Review application shall use equipment from a leading processors at minimum speed of 2.8 GHz from a leading manufacturer (including Intel or AMD); with a network-interface card with a minimum speed of 1GBPS; with a hard-disk drive with a minimum capacity of 250GB; with a high-end video card with 128MB RAM, 1024 x 768 screen resolution and highest 32-bit color quality.

5.4.7 VMS FUNCTIONS

a) Control Center Client Application

1. The VMS shall have a Control Center graphical user interface (GUI) that allows the user to efficiently configure and apply the following parameters, and perform the following procedures:
 - i. All camera configurations
 - ii. All recorder configurations
 - iii. All work schedules
 - iv. User and access rights and privileges, including rights for multisite configuration
 - v. Create schedules and apply them to specific camera groups
 - vi. Configure cameras and recorders individually, and as a group, in system components
 - vii. Preconfigure camera profiles (containing video quality configurations) to be managed and distributed as required in user defined logical groups
2. The user shall have the ability to add and edit interactive site plans and maps.
3. Control Center shall be controlled by access rights assigned by the system administrator, including:
 - i. Full access to all functions
 - ii. Limited to system configuration only
 - iii. Limited to Health Check viewing only
4. Control Center shall have the capability to automatically discover and perform initial IP camera configurations.
5. The VMS shall provide a health check single point of control mechanism to monitor operations and track system performance.
6. The VMS shall provide audit trails of activities performed in the system.
7. Control Center shall have the capability to provide a dashboard, with status information of each recorder that is part of a Master Server configuration.

b) Review Client Application

1. The VMS shall have a video viewing graphical user interface (GUI) that allows users to view live video, retrieve recorded video, and export video from a workstation PC.
2. The VMS Review application shall enable users to manage multiple windows and perform multiple tasks simultaneously. The VMS Review application includes the following functionality:
 - i. A quick video query button
 - ii. Ability to select time preference (AM/PM/2400Hrs)

- iii. Hot Function Keys
 - iv. Configurable playback speed in multiple increments up to 100x
 - v. The ability to retain time between queries
 - vi. The ability to view live or recorded video in multiple windows, including video from multiple Network Video Recorders and multiple sites
 - vii. Variable speed PTZ camera control (camera dependant)
 - viii. The ability to lock the PTZ control for a camera, depending on user rights and priority levels
 - ix. The ability to take-over a PTZ function, depending on user rights and priority levels
 - x. The ability to export video to digital media output devices, such as a CD, DVD, Blu-ray disk, and USB thumb drive, and to manage the exported files via an exported queue, depending on user rights.
 - xi. The ability to submit and manage multiple requests for video
 - xii. Support for time synchronized video playback on up to 16 windows simultaneously
 - xiii. Support for camera groups and maps that provide a video preview of the camera and alarm indication
 - xiv. Support for camera presets in a user-defined, multi-level tree structure. The following guidelines shall apply:
 - Each group has a user-defined name and user-defined contents
 - Cross-site monitor trees are supported for multisite environments
 - A group can contain cameras and/or other groups
 - Users can define multiple levels of groups and maps
 - A camera can be included in more than one group.
 - Users can select or drag-and-drop individual cameras to request video for playback or to open live video windows.
 - Guard Tours display sequential views of predefined workspaces created by the operator in the Review application, for specified periods of time.
 - Allow to synchronize playbacks video
 - Store the recent played video for quick playing
 - Ability to select playback played video from a recent playbacks list
3. The VMS shall allow the user to open, move, and size multiple, independent video windows as needed, including:
- i. Single windows
 - ii. 2 x 2: 4 (quad) windows, arranged in two rows of two windows each

- iii. 5 x1 window, arranged in one large window, surrounded by multiple tiles
 - iv. 3 x 3: 9 windows, arranged in three rows of three windows each
 - v. 4 x 4: 16 windows, arranged in four rows of four windows each
 - vi. A maximum layout of 8x8 windows
 - vii. Dynamic, flexible, and customizable layouts, including color skinning
 - viii. Up to 4 screens per workstations, for a maximum of 256 tiles @ CIF/5fps
 - ix. HD 16:9 support
- 4. The VMS shall support the ability to preserve aspect ratio.
- 5. The VMS shall support digital zoom on live or recorded video, without requiring a video pause.
- 6. The VMS shall enable/disable video de-interlacing.
- 7. Image Toolkit software shall include the following capabilities:
 - i. Adding the date and time to the image
 - ii. Adding text annotations to the image
 - iii. Copying the image to the clipboard so that it can be pasted into other applications
 - iv. Printing the image
 - v. Saving the image to disk in various standard file formats
 - vi. Adjusting the brightness and/or contrast of the image
 - vii. Converting a color image to gray scale
 - viii. Applying filters to the image to smooth or sharpen
 - ix. Applying edge detection to highlight borders and surfaces of objects within the image
- 8. The VMS Review application shall allow users to select any or all video tiles including live and recorded video for export from a precise user selectable start and end time with a single mouse click. The user shall also have the option to rename the target file name.
- 9. The VMS shall offer Investigation Management capabilities, including:
 - i. The ability to create an investigation from any multiple remote and local sites, depending on access rights
 - ii. The ability to include the following attachment types in the investigation binder:
 - 1. Live and recorded video
 - 2. Alarm video
 - 3. External files

- 4. Still images
 - 5. Video currently playing in the workspace
 - 6. Existing investigations
- iii. The ability to include explanatory notes in the investigation binder.
- iv. The ability to access and edit Investigations, depending on access right permissions.
- v. The ability to perform Investigation Management searches.
- vi. The ability to export Investigations and their attachments.
- 10. The VMS shall provide a default digital certificate (MD5) for signing exported video clips.
- 11. The VMS shall enable users to open live video windows, relative to the monitor capacity
 - i. Support serial or quad view
 - ii. Allow up to three (3) additional monitors to be configured per Review client to enable additional viewing capacity
- 12. The VMS shall support attaching video to documents, such as incident reports, and ease retrieval of reports and associated video.
 - i. Exported video format is .AVI
- 13. The VMS shall support video playback controls, including:
 - i. Speed Buttons to start and stop playback from the current video position
 - ii. Speed Buttons to step forward or backward through the video in single time increments
 - iii. Speed Buttons to step forward or backward through the video in single frame increments
 - iv. Speed Buttons to step forward or backward through the video in multiple frame increments
 - v. Speed Buttons for moving through video in reverse
 - vi. Ability to cause video to loop continuously
 - vii. Positioning controls, including a slider bar and buttons to quickly and conveniently position to the beginning, end, or any other time in the video clip
 - viii. Speed control, using a slider bar to control the rate of playback
- 14. The VMS shall support scanning recorded video for motion in all or specific Areas of Interest, and shall have the ability to set the motion sensitivity and sampling time.
- 15. The VMS shall authenticate video, enabling users to verify that the video has not been modified since it was recorded.

16. The VMS shall have live video windows consistent with video playback windows in appearance and operation.
17. The VMS shall allow the entire live video window to be a mouse-sensitive area for PTZ control.
18. The VMS shall provide an optional “heads up display” (HUD), which supports layering a PTZ control user interface over the video, providing a visual indication of the window areas that control zoom, focus, and iris functions.
19. The VMS shall support camera presets by providing a toolbar, or other GUI method, for working with camera presets when viewing live video from a PTZ camera.
20. The VMS shall provide the ability to view camera tours through a graphical, icon-based user interface.
21. The VMS shall allow the user to access a calendar view to query by month, day, and year, and by hour, minute, and second.
22. The VMS shall allow the user to access a hierarchical tree to manage the icons that represent cameras.
23. The VMS shall allow hovering from the camera list to preview the camera window in real-time.
24. The VMS shall provide auto-play alarm tiles and workspaces.
25. The VMS shall allow users to pin alarms to tiles, which keeps the alarm on the tile until it is acknowledged.
26. The VMS shall allow administrators to configure access rights and privileges for every user. The configured user access rights and privileges will apply when the user logs on to any workstation.
27. Review application operations shall be able to be restricted. It shall be possible to restrict or enable the following functionality:
 - i. Live video
 - ii. PTZ control
 - iii. Assigning PTZ priorities for take-over functionality
 - iv. Digital zoom
 - v. Camera menu
 - vi. Recorded video
 - vii. Export video
 - viii. Investigation management
 - ix. Alarm notification, alarm viewing, alarm history
 - x. Cameras
 - xi. Tours

- xii. Salvos
- xiii. Maps
- xiv. Sites

- 28. The VMS shall allow users to define, save, and call up PTZ presets, patterns, and virtual guard tours as supported by the camera manufacturer.
- 29. Integration with Physical Security
- 30. The VMS shall have certified integration with Physical Access Control Systems (PACS)
- 31. The VMS shall have certified integration with proposed Command and Control systems

c) Analytics Functions

- 1. The VMS analytics solution shall be a flexible architecture that allows use of analytics algorithms on IP cameras as well as encoders. The VMS analytics solution shall provide options for server based analysis.
- 2. Server based analytics shall be flexible enough to analyze streams from any camera being recorded by the VMS system. The Analytics server shall be capable of decoding and analyzing Meta data.
- 3. The VMS shall provide the ability to acquire and track an object within a predefined field of view, on selected cameras.
- 4. The VMS shall support object-based algorithms, and shall provide the following functionality:
 - i. Learn the scene
 - ii. Detect and track objects
 - iii. Adapt to a changing outdoor environment
 - iv. Ignore environmental changes including rain, hail, wind, swaying trees, and gradual light changes
 - v. Classify objects
 - vi. Detect tripwire events
 - vii. Detect multi-line tripwire events
 - viii. Detect “enters”, “exits”, “appears”, “disappears”, “inside of”, “loitering”, “leave behind”, and “taken away” events
 - ix. Detect scene change events
 - x. Create object size and size change filters
- 5. The VMS shall be able to combine object tracking with object classification, allowing detection of specific objects in a region of interest, while ignoring other object types.
- 6. The VMS shall support alarm generation and other actions, based on the VMS rule engine for when an object is detected, classified, and tracked.

7. The VMS shall support 3rd party facial recognition analytics and initiate an alarm event when a specific face is recognized from a user denied pre-configured list during a live video feed or in post event forensic analysis.
8. The VMS shall support 3rd party License Plate Recognition analytics and initiate an alarm event when a specific license number is recognized from a user defined pre-configured list during a live video feed or in post event forensic analysis.

d) Event Management

1. The VMS shall have a rule-based engine with powerful analytics capabilities that provides the following actions as responses to events and behaviors, including events that occur on one site and responses triggered on another site:
 - i. Automatic event notification
 - ii. Video distribution
 - iii. Process activation
2. Triggering responses shall be addressed on the following:
 - i. when an event occurs
 - ii. When two events occur within a specific time span
 - iii. When two identical and consecutive events occurs without another specific event occurring between the two
 - iv. When one event occurs without another event within a specific time span
3. The automated responses to behaviors shall be:
 - i. Trigger an alarm with 20 different alarm's priority, assigned to different users or monitors
 - ii. E-mail notification
 - iii. Assign a camera to a monitor
 - iv. Change output relay state
 - v. Call a camera preset
 - vi. Run a camera pattern
 - vii. Record on event
 - viii. Invoke an external application
 - ix. Output alarms to the Client SDK interface

e) Video Recording

1. The VMS Recorder shall be capable of performing multiple tasks simultaneously, and, provided hardware configuration and software setup guidelines are followed, no task shall interfere with any other task.
2. The VMS shall be able to perform the following tasks simultaneously:
 - i. Digitizing and compressing video, and calculating digital signatures for video authentication
 - ii. Writing video to files on local hard disks and maintaining an accurate index of the stored video files
 - iii. Deleting older video files as needed, freeing up space to record newer video files
 - iv. Selectively transferring recorded video to long-term storage media
 - v. Should support Storage on the edge: In case of network or NVR server failure the cameras should store the recording on the IP camera and once the network is restored back, the NVR server should synchronize and playback the video recording stored on the IP camera through VMS Client.
3. The VMS shall be capable of supporting dual streaming live or recorded video in different resolutions or frame rates. The VMS shall be capable of performing the following tasks related to alarms:
 - i. Executing video image analysis algorithms, including activity detection and video loss detection
 - ii. Receiving signals from alarm inputs and generating alarm messages
 - iii. Processing alarm response instructions including calling, changing recording modes, and controlling alarm relay outputs
 - iv. Forwarding alarms to a Review workstation, analog video monitor, or video wall
4. The VMS shall be capable of performing the following tasks and shall support the following recording modes:
 - i. Continuous recording. In the simplest mode, the Network Video Recorder units must record video 24 hours per day, 7 days per week, or as per user defined schedules.
 - ii. Event recording.
 - iii. Augment the recording quality based on an event.
 - iv. Selectively copy video to long-term storage or redundancy on archiving storage. System administrators shall be able to determine whether video will be retained on long-term storage media, for each continuous or scheduled recording instruction.

- v. Automatically retain video on long-term storage media when video is recorded as part of a defined response to an alarm event.
 - vi. Perform activity recording. The VMS shall support an event recording mode designed for handling activity detection events during periods when frequent activity is expected, but does not constitute an alarm event. Activity detection events shall be handled internally by the Network Video Recorders instead of triggering an alarm response. This mode preserves online video storage space by only retaining video in which activity has been detected.
 - vii. The VMS shall be capable of supporting multiple recorders, including the ability to: Add, modify, and remove recorders from the system
 - viii. Perform failover of recorders
 - ix. Perform dual recording from one camera source
 - x. Apply global recorder settings or edit existing individual recorder properties
 - xi. Define recording modes: centralized and distributed
 - xii. Associate cameras, recorders, and schedule assignments
5. The VMS shall support failover recording.
- i. The failover recorder shall act as a hot standby, ready to take over the functions of a primary Recorder. No action from the user shall be required.
6. The VMS shall support dual recording.
7. The VMS shall offer redundant recording which covers: Continuous recording during a recorder server failure (and access to recorded video) and or Recording in two different locations to address a catastrophic event by providing a simultaneous recording by two recorders, with independent (non-shared) video storage Enterprise Storage Manager (ESM)
- i. The VMS shall offer ESM servers for supporting long-term or off-site storage to any central disk storage device. It shall support any central disk storage device, including disk arrays with iSCSI connectivity and Storage Area Network (SAN) devices.
 - ii. The VMS ESM shall dynamically delete (groom) extraneous video from hard drives to make space for newer incoming video, based on specific retention parameters, while recognizing and preserving video clips marked by the system as important.
 - iii. The VMS shall seamlessly locate any requested video stored on disks or ESM servers, from any Review workstation.
 - iv. The VMS ESM shall automatically copy requested video from near online storage to online (disk) storage, easing video playback. When the user has finished reviewing the video, the VMS ESM shall retain the

online copy of the video to expedite processing of any subsequent requests for the same video.

f) Alarm Configuration

1. The VMS shall process alarms from a variety of alarm sources. Each type of alarm source shall have an “OFF” state (normal) and an “ON” state (triggered). The VMS shall monitor the state of alarm sources and generate alarm messages based on state changes.
2. The VMS system components shall provide alarm contacts to receive signals from electrical devices. Contacts are configurable as “normally open” or “normally closed”.
3. The VMS shall be capable of generating an alarm based on video image analysis, detecting activity through motion detection or object recognition in the areas of interest, or directional vectors. The absence of activity shall correspond to the “OFF” state of the alarm source; when activity is detected, the state of the alarm source shall be “ON”.
4. The VMS shall be capable of providing a way to define the areas of interest for activity detection for specific cameras.
5. The VMS shall be capable of enabling configurable activity detection sensitivity.
6. The VMS shall be capable of generating alarms when video loss is detected from the devices due to lost camera signals.

g) Alarm Responses

1. The VMS shall be able to configure scheduled alarm sources and responses, depending on the time of day and/or day of the week.
2. The alarm response shall consist of various types of instructions, to be executed by the VMS in response to an alarm message that can be generated by an alarm source.
3. The VMS shall support recording instructions for starting recording, or changing the recording mode, for one or more cameras connected to one or more Recorders.
4. The VMS shall support relay output instructions for controlling the state of one or more alarm relay outputs on Recorders, or other system components such as edge devices or IP cameras.
5. The VMS shall trigger contact closures on edge devices or IP cameras that are hardware equipped with this capability.
6. The VMS shall be able to display text messages to users at the alarm monitoring station.
7. The VMS shall be able to display/send an alarm message to the Application Programming Interface for the Client SDK.

h) Video Storage Recorder Management

1. The VMS shall be capable of managing online recorder storage. Storage shall be intelligently managed so that the video most likely to be requested by users will be retained online.
2. The VMS shall be capable of circular overwrites, and online storage on the recorder units shall be managed on a continuous circular overwrite basis.
3. The VMS shall be capable of event recording and selective online storage.
4. The VMS shall be capable of retaining non-event video online for a minimum amount of time, depending on the recorder hard disk space.
5. The VMS shall be capable of retaining video online after transferring it to long-term storage (ESM). Video shall be retained online on the recorder to support immediate playback, even if the video has been successfully copied to long-term storage media.

i) Managing Long-Term Storage and Archiving

1. The VMS shall support automatic long term storage with the ESM.
2. Long-term storage shall be implemented using separate storage attachments.
3. The VMS shall support multiple long-term storage devices.
4. The VMS shall be capable of independent operations between storage servers.
5. The VMS shall be capable of immediate transfer to long-term storage.
6. The VMS shall support the ability to “catch up” after storage server downtime. If a storage server must be taken out of service temporarily for maintenance, the VMS shall retain video designated for long-term storage online on Recorders. When the storage server is placed back in service, it shall transfer video data to long-term storage faster than the rate at which new video is being recorded.
7. The VMS shall be capable of variable retention times, i.e., it shall support the segmentation of cameras into groups based on the video retention requirements, so that video is retained for some cameras longer than for others.

j) Archived and Bookmarked Video

1. The VMS shall allow disks to be reserved for video archiving.
2. The VMS shall support copying bookmarked video to the appropriate archive storage media, and ensure that the video will not be overwritten or deleted for the specified number of days.
3. The VMS shall allow any video clip attached to an investigation to be automatically archived. The default video retention time shall be 60 days. This retention period can be modified by the system administrator.
4. The VMS shall allow database queries to find reports, view reports, and export an HTML page with the ability to attach video clips and still images to a report.

k) Health Check

1. The VMS shall provide a Health Check application for live monitoring and detailed system performance metrics on system components, including all server-side software applications, including video recorder software.
2. The VMS shall provide a Health Check application for live monitoring and detailed system performance metrics on edge devices, and IP cameras.
3. The VMS shall be capable of exporting performance analysis results.
4. The VMS shall offer a user interface designed to enable the management of the following:
 - i. System logs
 - ii. System alerts
 - iii. Audit trail
 - iv. Performance
 - v. Recorder sanity, through a dashboard Redirection to various outputs, such as Windows event logs and e-mail
5. The VMS shall be capable of capturing real-time performance analysis.

l) Audio

1. The VMS shall support including audio in the video stream. The VMS supports unidirectional synchronized audio support for live and playback video, and allows for the following functions:
 - i. Exporting audio together with the video
 - ii. Audio support with the Virtual Matrix
 - iii. Audio support using the Client SDK
 - iv. Compression modes, including: PCM, ULAW, GSM, depending on the edge device capabilities

m) Camera Tampering Detection

1. The VMS shall support the Camera Tampering Detection resident on the edge devices. The VMS shall monitor the following types of tampering alerts communicated by the edge devices:
 - i. Camera blocked fully or partially
 - ii. Out of Focus (OoF) or Camera Defocus, where the image becomes blurred because the camera is being defocused

n) USB Keyboard Integration

- i. Support PTZ Joystick in Review, Support full USB Keyboard for the video wall, Control PTZ of the selected tile, Switch tile, Quick Query & Back to Live

6. CALENDAR OF EVENTS

The following table enlists important milestones and timelines for completion of EOI Processing activities:

Sl. No	Milestone	Date and time (dd-mm-yyyy; hh:mm)
1	Release of Expression of Interest (EOI)	21/09/2015
2	Last date for submission of written questions by Firms	02/10/2015 (up to 1500 hrs)
3	Response to the Queries	07/10/2015
4	Last date for Submission of EOI Response	15/10/2015 (up to 1500 hrs)
5	Opening of EOI Responses	16/10/2015 (1100 hrs)
6	Declaration of Short listed Firms	20/10/2015

7. EXAMINATION OF THE “EOI DOCUMENTS”

The Firms are expected to examine all instructions, forms, terms, project requirements and other details in the “EOI documents”. Failure to furnish complete information as mentioned in the “EOI documents” or submission of a proposal not substantially responsive to the “EOI documents” in every respect will be at the Firm's risk and may result in rejection of the proposal.

8. VENUE and DEADLINE FOR SUBMISSION OF PROPOSALS

Proposals, in its complete form in all respects as specified in the EOI, must be submitted to ECIL at the following address:

TEHNICAL MANAGER (PURCHASE),

ISG, ECIL, Hyderabad - 500062

Telephone: 040-27182655

Fax: 040-27122540

Email: igmmgt@ecil.co.in

ECIL may, in exceptional circumstances and at its discretion, extend the deadline for submission of proposals by issuing an addendum to be made available on the ECIL's website. In such a case, all rights and obligations of ECIL and the Firms will thereafter be subject to the deadline as extended.

Brief about EOI:

Sl.No	Item	Description
1	Project Title	Selection of OEM for customization, supply and integration of <i>Video Analytics Integration Platform (VAIP)</i>, with <i>Video Content Analytics (VCA)</i> & <i>Video Surveillance System (VMS)</i>
2	Project Initiator Details	Sr.DGM (Materials), ISG, ECIL, Hyderabad
3	Department	Security Systems and Projects Division, Instruments and Systems Group
4	Contact Person (for commercial queries)	TEHNICAL MANAGER (PURCHASE), ISG, ECIL, Hyderabad - 500062 Telephone: 040-27182655 Fax: 040-27122540 Email: igmmgt@ecil.co.in
5	Contact Person (for technical queries)	Sr. Dy. General Manager (Projects) SSPD/ISG, ECIL, Hyderabad - 500062 Telephone: 040-27182880 Fax: 040-27121611, 27125588 Email: prasad_p@ecil.co.in
5	Website	http://www.ecil.co.in

9. ELIGIBILITY AND PREQUALIFICATION CRITERIA

9.1 CONDITIONS UNDER WHICH THIS EOI IS ISSUED

- i) This EOI is not an offer and is issued with no commitment. ECIL reserves the right to withdraw the EOI and change or vary any part thereof at any stage. ECIL also reserves the right to disqualify any Firm, should it be so necessary at any stage.
- ii) ECIL reserves the right to withdraw this EOI if ECIL determines that such action is in the best interest of the corporation.

iii) Short-listed Firms would be issued formal tender enquiry/Request for Proposal inviting their technical and commercial EOIs at a later date.

iv) Timing and sequence of events resulting from this EOI shall ultimately be determined by ECIL.

v) No oral conversations or agreements with any official, agent, or employee of ECIL shall affect or modify any terms of this EOI and any alleged oral agreement or arrangement made by a Firm with any department, agency, official or employee of ECIL shall be superseded by the definitive agreement that results from this EOI process. Oral communications by ECIL to Firms shall not be considered binding on ECIL, nor shall any written materials provided by any person other than ECIL.

vi) Neither the Firm nor any of the Firm's representatives shall have any claims whatsoever against ECIL or any of their respective officials, agents, or employees arising out of, or relating to this EOI or these procedures (other than those arising under a definitive service agreement with the Firm in accordance with the terms thereof).

vii) Applicants who are found to canvass, influence or attempt to influence in any manner the qualification or selection process, including without limitation, by offering bribes or other illegal gratification, shall be disqualified from the process at any stage.

viii) Each applicant shall submit only one Pre-qualification requirements proposal.

9.2 RIGHTS TO THE CONTENT OF THE PROPOSAL

For all the proposals received before the last date and time of EOI submission, the proposals and accompanying documentation of the Pre-Qualification proposal will become the property of ECIL and will not be returned after opening of the pre-qualification proposals. ECIL is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the Firms. ECIL shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

9.3 ACKNOWLEDGEMENT OF UNDERSTANDING OF TERMS

By submitting a proposal, each Firm shall be deemed to acknowledge that it has carefully read all sections of this EOI, including all forms, schedules and annexure hereto, and has fully informed itself as to all existing conditions and limitations.

9.4 EVALUATION OF PRE QUALIFICATION PROPOSAL

The Firms' Pre-Qualification Proposal in the "EOI document" will be evaluated as per the requirements specified in the EOI and adopting the pre-qualification criteria spelt out in this EOI. The Firms are required to submit all required documentation in support of the pre-qualification criteria specified (e.g. detailed product citations and completion certificates, client contact information for verification, profiles of project resources and all others) as required for evaluation.

9.5 LANGUAGE OF PROPOSALS

The proposal and all correspondence and documents shall be written in English.

9.6 PRE-QUALIFICATION CRITERIA

The invitation for EOI is open to all entities registered in India who fulfill prequalification criteria as specified below:

Criteria Requirement	Documents Submission Requirements
Resources and strength	
The bidder should be a Company registered under Companies Act, 1956 in India / firm registered in India and should be registered with the Service Tax Authorities.	Copy of Certificate of Incorporation/certificate of firm registration and Copy of Central Sales Tax certificate, VAT, PAN & Service Tax Registration Certificates
The bidder should be an individual organization. Consortium shall not be allowed.	Certificate from the authorized signatory of the bidder.
<p>The Bidder should be an OEM having a “Video Analytics Integration Platform (VAIP)” with integrated Control & Command Centre. The VAIP must be capable of integrating any industrial standard third party systems like:</p> <ol style="list-style-type: none"> 1. IP based Surveillance system 2. Access Control System 3. Fire Alarm System 4. Tetra Radio Integration System 5. Power Fence System 6. License Plate Recognition System 7. Panic Alarms 8. Glass Break and 9. Gun Shot Detection Sensors. <p>The Bidder must be in business for last 3 years and should have after sales service centers in India and the support facilities should be fully owned by the Bidder and managed by its employees.</p>	Certificate from the authorized signatory of the bidder. A copy of product catalogue/ datasheet/ technical literature must be invariably enclosed with the bid.
The bidder should have at least 1000 full time employees (in India or abroad), out of which at least 100 should be part of CCTV/Biometric	Certificate from In-charge / Head, HR certifying total strength and no. of resources dedicated for CTV/Biometric

Criteria Requirement	Documents Submission Requirements
analytics development, working in India.	analytics development work in India.
At least 02 (VAIP) installations with 800 inputs & 01 installation of 300 IP camera of the offered make should have been successfully supplied & installed by the Bidder in India or abroad with at least one installation in India.	Copy of the installation certificate
The Bidder should have earlier experience or should be currently in the process of executing large turnkey projects for a Central / State Government Organization in India	Work order copy to be produced
<p>The bidder should have implemented at least one Integrated Video Analytics assignment covering minimum 300 Camera (Digital and Analog) with minimum three areas/ scenario identified below:</p> <ul style="list-style-type: none"> a. Crowd detection b. Left baggage detection c. Face recognition d. Intrusion detection (at perimeter) e. Counter flow of vehicles f. Illegal parking 	Work order copy to be produced
The bidder should have IP rights for proposed Integrated Video Analytics Platform / Solution.	Certificate from authorized signatory
The bidder should not currently have been blacklisted by any Government Agency or under a declaration of ineligibility for fraudulent or corrupt practices or inefficient/ineffective performance.	Certificate from authorized signatory
The bidder should be prepared for joint collaboration / development with ECIL so as to meet additional analytics requirement or futures needs which are otherwise not part of original Analytics Integration Platform and must share APIs, SDKs and other technical documents relevant to the proposed application and provide necessary	An undertaking from the authorized signatory.

Criteria Requirement	Documents Submission Requirements
assistance/support/training to ECIL engineers for further up-gradation/enhancement of the application or for integration with other applications.	
Annual Turnover and Net Worth:	
The bidder's annual turnover towards CCTV business / solution should be at least Rs 100 crores in each of the last three financial years (2012-13, 2013-14, 2014-15).	Duly certified statement from appointed statutory auditor for the last three financial years indicating the amount of turnover during these years.
The bidder's net worth should be positive for each of the last three financial years (2012-13, 2013-14 & 2014-15)	Duly certified statement from appointed statutory auditor for the last three financial years indicating the amount of turnover during these years.
Certification:	
The bidder responsible for product customization and implementation should have a SEI CMMi (Capability Maturity Model) level -3 or higher certification.	Valid copy of the Certificate as on the last date of submission of bid.
OFFICES / DEVELOPMENT CENTER	
The bidder should have Development center in India.	Declaration by authorized signatory.

Note: EOI Proposals must accompany documentary evidence in support of the above eligibility criteria and proposals submitted without supporting documents will be summarily rejected.

Firms fully meeting the above criteria only will be qualified for issue of RFP/tender.

In case of long duration projects that includes operations and maintenance services in scope, it is expected that the Firm has successfully completed deployment and 'GO LIVE' phase in the project.

In respect of the cited projects, the Firm must be directly responsible for the implementation of the projects and not just a member of a consortium.

Only Project Citations completed / started in the last 3 financial years (2012-13, 2013-14 & 2014-15) will be considered for evaluation.

9.7 RESPONSE REQUIREMENTS

- (i) Proposals must be direct, concise, and complete. All information not directly relevant to this EOI should be omitted.
- (ii) A Firm shall not participate in more than one EOI. The Firm shall ensure, directly or indirectly, not to either participate or not be involved with multiple EOIs, which will lead to disqualification of all EOIs in which the Firm is involved.
- (iii) The Pre-Qualification Proposal shall be sealed and super scribed “Response to Pre-Qualification Requirements – EOI for **Selection of OEM for customization, supply and integration of Video Analytics Integration Platform (VAIP), with Video Content Analytics (VCA) & Video Surveillance System (VMS)**” on the top right hand corner and addressed to ECIL at the address specified in this document.
- (iv) The pre-qualification proposal should be submitted with two printed copies of the entire proposal, one marked ORIGINAL and the second one as DUPLICATE and a soft copy on non-rewriteable DVD with all the contents of the pre-qualification proposal. The words “Response to Pre-Qualification Requirements – EOI to work as Business Partners for implementing **“IP based Video Analytics Integration Platform (VAIP), Video Content Analytics (VCA) & Video Surveillance System (VMS)”**” shall be written in indelible ink on the DVD. The Hard Copy shall be signed by the authorized signatory on all the pages before being put along with the DVD in the envelope and sealed.
- (v) In case of discrepancies between the information in the printed version and the contents of the DVDs, the printed version of the pre-qualification proposal will prevail and will be considered as the proposal for the purpose of evaluation.
- (vi) The proposal should contain the copies of references and other documents as specified in the EOI.
- (vii) A broad resolution/Power of Attorney authorizing the Firm’s representative to sign/ execute the proposal as a binding document and also to execute all relevant agreements forming part of EOI shall be included in this envelope.
- (viii) ECIL will not accept delivery of proposal in any manner other than that specified in this EOI. Proposal delivered in any other manner shall be treated as defective, invalid and rejected.

9.8 PRE-QUALIFICATION REQUIREMENTS PROPOSAL

The Pre-Qualification Proposal should be submitted in the sealed envelope with the following details. Firms are requested to submit their responses for the Pre-Qualification Requirements in five (5) parts, clearly labeled according to the following categories:

9.8.1 Part I – Covering Letter and Board Resolution/Power Of Attorney (PoA)

- a. Covering Letter from the Firm as per the format provided in Annexure – Form I

- b. Board resolution/Power Of Attorney authorizing the Firm's representative to sign/ execute the EOI proposal and execute all relevant agreements forming part of EOI.

9.8.2 Part II – Details of the Organization

- a. This part must include a general background of the respondent organization (limited to 400 words) along with other details of the organization as per Annexure-FORM II.
- b. Vendor registration form (which can be down loaded from ECIL Web site (www.ecil.co.in) duly filled in along with necessary supporting document.
- c. Copy of registration certificate of the company.
- d. Certificate from the authorized signatory of the Firm certifying that the Firm is an individual organization and not a consortium.
- e. Financial details concerning the organization as per Annexure-FORM III, accompanied with duly certified statements from appointed statutory auditor for the last three financial years indicating the amount of turnover towards **CCTV business / solution** for each of the last three financial years (2012-13, 2013-14 and 2014-15) and net worth of the firm during these years.
- f. Valid copy of the SEI CMMi (Capability Maturity Model) level -3 Certificate or higher
- g. Copies of the VAT/ PAN / ITCC / Service tax certification attested by a Notary / auditor.
- h. A declaration on a Non-judicial stamp paper of Rs 100/- from the authorized signatory confirming that the firm is neither blacklisted nor debarred by any Govt. agency for fraudulent or corrupt practices or inefficient performance.

9.8.3 Part III – Relevant Project Experience

Copies of the purchase orders executed and Installation and Commissioning certificates in support of eligibility requirements listed in section 11.6 above at sr no. (f), (g) and (h) (as per form given in the "EOI document").

9.8.4 Part IV – Proof of Fulltime CCTV/IT Professionals in the Firm's Organization

Certificate from In-charge / Head, HR certifying total strength and no. of resources dedicated for CCTV/Biometric analytics development work in India.

9.8.5 Part V – Product/Project Details

- a. Certificate from the authorized signatory of the Firm certifying that the Firm is an OEM for the product/offered solution. A copy of product catalogue/ datasheet/ technical literature must be invariably enclosed with the EOI.
- b. An undertaking from the authorized signatory confirming possession of IP rights for the proposed solution.
- c. An undertaking from the authorized signatory confirming the readiness of the firm to work with ECIL for joint development by sharing APIs, SDKs and any other technical documents required for further up-gradation/enhancement of the application or for integration with other applications.
- d. Clause by Clause compliance to the scope of work.

10. RFP Bid Evaluation Methodology:

Bids will be evaluated in following FOUR stages:

(A) Pre-qualification:

- (i) At first stage, the proposal shall be evaluated to ascertain whether it fulfils the criteria for responsiveness.
- (ii) Thereafter, the proposals would be checked for the pre-qualification criteria.

(B) Technical Evaluation:

- (iii) The proposals which meet the criteria of responsiveness and also that of pre-qualification will be evaluated for ascertaining the Technical score of the proposal.
- (iv) The technical evaluation will be carried out by a technical evaluation committee constituted by the competent authority and will be based on a well-defined technical evaluation criteria and will cover different aspects like financial soundness, technical abilities, resource profile, relevant past experience and assessment of proposed approach by seeking presentation/demonstration etc.
- (v) The minimum qualifying score at the stage of Technical Evaluation of Proposals will be 70 out of 100.

(C) Price Bid Evaluation:

- (vi) Price bids of those bidders whose technical bids have scored 70 or more marks will be opened.
- (vii) Price bids that are less than 50% of the average bid price will be disqualified (the average bid price is computed by adding all Price bid values of ALL the qualified bidders and dividing the same by the number of bidders).
- (viii) Amongst the bidders whose bid is equal to Or higher than 50% of average price bid as defined above, the lowest (L1) bidder will be awarded 100% score. Financial scores of other bidders will be evaluated using following formula:
Financial Score (Fs) = {(Price proposal of L1 bidder/Commercial Bid of the other Bidder) X 100}%

(D) Combined Evaluation:

- (ix) The financial and technical scores secured by each bidder will be added giving weightage of 30% and 70% respectively to compute a Composite Bid Score.
- (x) **The bidder securing the highest Composite Bid Score will be adjudicated as the most responsive and Highest Ranking Bidder for award of the Project.**
The overall score will be calculated as follows:-
$$Bs = 0.30 * Fs + 0.70 * Ts$$

Where
Bs = overall score of bidder
Ts = Technical score of the bidder (out of maximum of 100 marks)
Fs = Normalized financial score of the bidder

11. Due Diligence

The Firm is expected to examine all instructions, forms, terms and conditions, and specifications that are provided in the "EOI document". The EOI should be precise, complete and in the prescribed format as per the requirement(s) of the "EOI document". Failure to furnish all information required by the EOI document or submission of a EOI not responsive to the 'EOI document' in every respect will be at the Firm's risk and may result in rejection of the proposal.

The Firm shall bear all costs associated with the preparation and submission of its EOI and ECIL will not be in any case held responsible or be liable for these costs, regardless of the outcome of the EOI Process.

12. Validity of the EOI Proposal

The Firms have to confirm the validity of the proposal for 2 months (60 days) from the last date of submission of proposal.

13. Clarification to "EOI documents"

In the event that any Firm requires any clarification on the EOI document, such Firms are expected to send their queries to ECIL in writing by email only to igmmgt@ecil.co.in on and before the closing date for EOI submission, clearly stating the subject as "Selection of solution Provider to work as Business Partners for implementing ***"IP based Video Analytics Integration Platform (VAIP), Video Content Analytics (VCA) & Video Surveillance System (VMS) "*** to enable ECIL to have adequate notice of the said queries so that the same may be addressed and the response/clarifications to the queries can be hosted on ECIL website: www.ecil.co.in

Nothing in this section shall be taken to mean or read as compelling or requiring ECIL to respond to any questions or to provide any clarification to a query. ECIL reserves the right not to respond to questions it perceives as non-relevant which a Firm may raise, or not to provide clarifications if, ECIL in its sole discretion, considers that no reply is necessary.

It is the responsibility of the Firm to confirm the receipt of the queries to ECIL.

No extension of Deadline for Submission of EOI Proposal will be granted on the basis or grounds that ECIL has not responded to any question or provided any clarification to a query.

14. Confidentiality

The Firm shall keep all information confidential related to this EOI (including the tender document) with the same degree of care as it would treat its own confidential information. The Firms shall note that the confidential information will be used only for

the purposes of this EOI and shall not be disclosed to any third party for any reason whatsoever.

As used herein, the term "Confidential Information" means any written information, including without limitation, information created by or for the other party, which relates to internal controls, computer or data processing programs, algorithms, electronic data processing applications, routines, subroutines, techniques or systems, or information concerning the business or financial affairs and methods of operation or proposed methods of operation, accounts, transactions, proposed transactions or security procedures of either party or any of its affiliates, or any client of either party, except such information which is in the public domain at the time of its disclosure or thereafter enters the public domain other than as a result of a breach of duty on the part of the party receiving such information. It is the express intent of the parties that all the business process and methods used by the Firm in rendering the services hereunder are the Confidential Information of the Firm.

At all times during the performance of the Services, the Firm shall abide by all applicable ECIL security rules, policies, standards, guidelines and procedures. The Firm should note that before any of its employees or assignees is given access to the Confidential Information, each such employee and assignees shall agree to be bound by the term of this EOI and such rules, policies, standards, guidelines and procedures by its employees or agents.

The Firm should not disclose to any other party and keep confidential the terms and conditions of this EOI, any amendment hereof, and any Attachment or Annexure hereof.

The obligations of confidentiality under this section shall survive rejection / termination / expiry of the contract for a period of ten years.

15. Language of EOI

The EOI prepared by the Firm, as well as all correspondence and documents relating to the EOI exchanged by the Firm and ECIL shall be written in English language only.

However, in case Firm chooses to enclose certain supporting document(s) in any language other than English, then Firm shall also enclose certified authenticated translated copies of the same in English language. Any document, which is not translated into English, will not be considered. For the purpose of interpretation and evaluation of the EOIs, the English language translation shall prevail.

ANNEXURE –FORM-I

To
Sr. DGM (Materials),
Electronics Corporation of India Limited
SSPD/ISG,
ECIL Post
Hyderabad-500062

Dear ,

Ref:- INVITATION FOR EXPRESSION OF INTEREST (EOI) FOR “Business Partners for implementing
“IP based Video Analytics Integration Platform (VAIP), Video Content Analytics (VCA) & Video Surveillance System (VMS) ”

Having examined the Expression of Interest (Eoi), the receipt of which is hereby duly acknowledged, we, the undersigned, intend to submit a Pre-qualification requirements proposal in response to the Expression of Interest (Eoi).

We attach hereto the response as required by the Eoi, which constitutes our proposal.

Primary and Secondary contacts for our company are:-

	Primary Contact	Secondary Contact
Name:		
Title:		
Company Name:		
Address:		
Phone:		
Mobile:		
Fax:		
email:		

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to ECIL, is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead ECIL in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the short listing process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so.

We agree for unconditional acceptance of all the terms and conditions set out in the Eoi document.

It is hereby confirmed that I/We are entitled to act on behalf of our company/corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2015.

(Signature) (In the capacity of)

(Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company) Seal/Stamp of Firm

Witness Signature:

Witness Name:

Witness Address:

CERTIFICATE AS TO AUTHORISED SIGNATURES

I, the Company Secretary of, certify thatwho signed the above EOI is authorized to do so and bind the company by authority of its board/governing body.

Date:

Signature:

(Company Seal)

(Name)

2. FORM II: GENERAL DETAILS OF THE ORGANIZATION

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business in India	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	
Address of the Registered Office in India	
Other Relevant Information	
Mandatory Supporting Documents:	
<p>Certificate of Incorporation from Registrar of Companies (ROC)/Certificate of registration of firm. Relevant sections of Memorandum of Association of the company or filings to the stock exchanges to indicate the nature of business of the company.</p>	

3. FORM III: FINANCIAL DETAILS OF THE ORGANIZATION

Financial Information			
	FY 2012-13	FY 2013-14	FY 2014-15
Revenue (in INR crores)			
Profit Before Tax (in INR crores)			
Revenue from CCTV business / solution (in INR crores)			
Other Relevant Information			
Mandatory Supporting Documents :			
<p>Auditor Certified financial statements for the last three financial years; 2012-13, 2013-14 & 2014-15 (Please include only the sections on P&L, revenue and the assets, not the entire balance sheet.) Certification by the company auditors supporting the revenue break-up towards CCTV business / solution.</p>			

4. FORM IV: TURNKEY CCTV PROJECT EXPERIENCE

Transitioning of Turnkey CCTV Project Experience	
General Information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Current Status	
Project Details	
Description of the project	
Geographical Scope	
Outcomes of the Project	
Scope of Transition	
Business Processes	
Applications	
Technologies Used	
Infrastructure	
Operations & Services	
Number of Location/Sites	
Other Details	
Due-Diligence During Transition	Y/N Indicate the duration in case there was a due-diligence performed before the selection process.
Duration of Transition(post selection)	
Total Duration of the project (no. of months, start date, completion date)	
Total cost of the project	
Total cost of the services provided by the Firm	
Other Relevant Information	
Mandatory Supporting Documents: Letter from the client duly indicating the salient points like cost, period, scope of services like software, hardware, networking, O&M etc and successful completion of the project.	
Project Capability Demonstration	
Complete details of the scope of the project shall be provided to indicate the relevance to the pre-qualification criterion (which is part of minimum qualification criteria).	