Request for Proposal

for

Garrahy Courthouse Garage
Electronic Security Systems

Rhode Island Convention Center

1 Sabin St, Providence, RI 02903

Issued: December 2019

Important Dates

RFP Release	December 18, 2019
Pre-bid Conference / Walkthrough	January 6, 2020 at 10 AM
Deadline for submitting questions	January 8, 2020 at 10 AM
Proposal Due Date	January 17, 2020 at 10 AM

Prepared by:

Broad Reach
100 Folly Landing
Warwick, RI 02886
(401) 885-4848
broadreachnetworks.com

GSC
SECURITY
CONSULTING
80 Woodland Road
North Smithfield, RI 02896
Phone (508) 838-6180
gristsecurityconsulting.com

Table of Contents

1 General

1.1 SCOPE

1.1.1 The Rhode Island Convention Center (RICC) is seeking proposals from interested vendors to furnish and install new video surveillance, management, and access control systems to serve the new Garrahy Courthouse Parking Garage at 75 Clifford Street, Providence, RI 02903.

1.1.2 Vendors must include all necessary civil, electrical, mechanical, and administrative services, and provide all equipment and services related to the design, installation, setup, testing, and maintenance of the proposed systems.

1.2 PROPOSAL DUE DATE

1.2.1 SEALED PROPOSALS shall be submitted no later than 10:00 AM, E.S.T. on January 17, 2020, at which time they will be opened and acknowledged. Responses received after that time and date will be returned unopened. The Respondent shall assume full responsibility for timely delivery at the location designated for the receipt of Responses.

1.2.2 Four (4) printed proposals plus one (1) electronic version (on USB Memory Stick) shall be delivered to the attention of:

Howard Allen
Complex Purchasing Manager
Rhode Island Convention Center
1 Sabin Street
Providence, RI 02903

1.2.3 Please label submissions with respondent’s name and address, the bid due date, and title: **“Garrahy Garage ESS”**

1.3 PRE-BID WALKTHROUGH

1.3.1 There will be a **MANDATORY** pre-proposal conference at the Garrahy Garage, 75 Clifford Street, Providence, RI 02903 on January 6, 2020 at 10:00 AM. A briefing will take place, followed by a site tour of existing conditions with Q+A. Note that the Garrahy Garage is still under construction, so please bring a hard hat.

1.3.2 Respondents are asked to pre-register by sending the names and contact info of any personnel planning to attend the pre bid to Broad Reach, via e-mail at SPECS@BRNX.COM. You will receive a response with the exact location of the pre-bid and any updated documentation.

1.4 IMPORTANT DATES

RFP Release	December 18, 2019
Pre-bid Conference / Walkthrough	January 6, 2020 at 10 AM
Deadline for submitting questions	January 8, 2020 at 10 AM
Proposal Due Date	January 17, 2020 at 10 AM

1.5 DEFINITIONS

1.5.1 Request for Proposal (RFP) Consists of this RFP, the Invitation to Bid, the Vendor Qualifications form, as well as any addenda that may be released prior to the bid submission deadline.

1.5.2 A Response is a complete and properly signed proposal to do the Work as stipulated therein, submitted in accordance with the RFP.

1.5.3 The terms respondent, vendor, bidder, contractor and offeror used herein all refer to the vendor submitting a response to this RFP. The term Customer refers to the party that is seeking bids for services under this RFP. The terms bid and response are synonymous.

1.5.4 Financial Terms means the amount of compensation to be received by Vendor as evidenced by the Contract Documents, during the contract time.

1.5.5 Work is the services to be performed by the successful Respondent as outlined in the Scope of Work.

1.5.6 The Rhode Island Convention Center Authority (RICCA) is the governing office that oversees the management of the Rhode Island Convention Center.

1.5.7 The Garrahy Garage and the Rhode Island Convention Center are the locations where the work is to be performed.

1.5.8 SMG is the business firm that manages the Garrahy Garage, Rhode Island Convention Center, and Dunkin' Donuts Center for the Rhode Island Convention Center Authority.

1.6 TERMS OF USE / CONFIDENTIALITY

1.6.1 This document is to be used only by the recipient to assist in responding to the project for which it is intended.

1.6.2 Any other use or reproduction, in whole or in part, is prohibited without the written permission of the author.

1.6.3 Documents and information received by the Contractor(s) are confidential and shall be treated as such by the Contractor(s). Contractor(s) shall hold in confidence and protect the documents and information contained therein, to prevent any unauthorized use and dissemination to others.

1.6.4 Documents and information received by the Contractor(s) shall only be distributed and discussed with persons directly involved in the preparation of the Contractor(s) response to this RFP.

1.6.5 After award is made, non-successful Contractor(s) shall return to owner all documents and information received and destroy all paper copies and electronic versions and files.

1.7 PROPOSAL COSTS

1.7.1 All costs associated with developing or submitting a response to this solicitation, or to provide oral or written clarification of its content, shall be borne by the offeror. The Customer assumes no responsibility for these costs.

1.8 MODIFICATIONS TO RFP

1.8.1 The Customer reserves the right to revise, modify, supplement, or withdraw this RFP at any time. In the event that it becomes necessary or desirable to revise, modify, supplement, or withdraw any part or all of this RFP, an addendum to this RFP or other notification will be issued.

1.9 SUBMISSION MATERIALS

1.9.1 All materials submitted regarding this RFP will become the property of the Customer and will only be returned to the vendor at the Customer's option. Responses may be reviewed by any person or persons at the discretion of the Customer. The Customer reserves the right to use any RFP ideas or options presented in reply to this request. Disqualification of a vendor or non-acceptance of the RFP does not eliminate this right.

1.10 INSURANCE REQUIREMENTS

1.10.1 Vendor is required to maintain insurance as described herein for the duration of the project.

1.11 SCHEDULES

1.11.1 To assure adequate planning and execution so that the work is completed within the number of calendar days allowed in the Contract, vendor will prepare and maintain schedules and reports. Vendor will graphically show the order and interdependence of all activities necessary to complete the work, including responsible party, and the sequence in which each activity is to be accomplished. Submit this schedule / work plan as part of vendor response.

1.11.2 Further scheduling and reporting requirements (for the successful vendor only) are detailed under implementation.

1.12 PROPOSAL VALIDITY

1.12.1 Responses are considered to be irrevocable for a period of not less than 90 days following the opening date, and may not be withdrawn, except with the express written permission of the purchasing agent of the Customer.

1.12.2 All pricing submitted will be considered to be firm and fixed unless otherwise indicated herein.

1.13 RESPONSE FORMAT

Responses should be organized in the following manner:

1.13.1 Section 1: RFP Response

1.13.1.1 RFP Exceptions Lead Sheet- Include a list of any specifications to which Contractor does not agree or comply, with brief explanation. (More detailed explanation should appear in the appropriate section).

1.13.1.2 Vendor will follow the format set forth by this RFP, responding to each paragraph individually. Information should be provided under its appropriate paragraph as requested.

1.13.1.3 For those paragraphs that do not require extensive response, vendor should respond with, for example, “Acknowledged and will comply”.

1.13.1.4 Attach Datasheets for each system component (hardware and software).

1.13.2 Section II: Cost Information

1.13.2.1 In addition to the paragraph-by-paragraph response, the vendor shall include, as a distinct section in vendor response labeled "Cost Information", the detail of the various components of the system(s) proposed with their associated costs. Include subtotals where appropriate, and a total cost.

Add alternates, where requested, should be itemized and totaled separately.

Cost information should be itemized as fully as possible, as this will assist Customer in comparing the different vendor solutions.

1.13.2.2 Be sure to include all costs, software license fees, support costs, and any fees, such as permits, certification fees, freight, one time install, or any other administrative or governmental surcharges or fees.

1.13.2.3 Provide normal and off-hours labor rates that would be charged to customer for ongoing move-add-change activity.

1.13.3 Section III: Include the following Company Information:

1.13.3.1 Company History/Qualification. Provide a detailed history of Respondent and a statement of qualifications including a description of comparable services provided for comparable projects including dates.

1.13.3.2 Financial Qualifications. Provide evidence that Respondent has the financial ability to perform the Work. Respondent must provide their last two (2) financial statements. In the case of a subsidiary, statements must be on the operating entity. No statement of the parent or holding company is acceptable.

1.13.3.3 If the Respondent is a Minority Business Enterprise certified by the Rhode Island Department of Economic Development, the Response should so indicate.

1.13.3.4 References and qualifications: Complete the Bidder Qualification Forms (attached in Appendix A).

1.13.4 Additional information such as marketing and sales brochures are welcomed but are in no way a substitute for the information format requested in the RFP.

1.13.5 Non-conformance to the format requested may result in rejection of vendor's proposal.

1.14 RESPONSE ATTACHMENTS

1.14.1 If there is a general purchase and sale agreement or other form contract that Contractor will expect Customer to execute, this should be included with the proposal. Requests for executing form contracts after award may be refused.

1.14.2 Each copy of the Response shall include the legal name of the Respondent and a statement identifying the Respondent as a sole proprietor, partnership, corporation or other legal entity as appropriate. Each copy shall be signed by the person or persons legally authorized to bind the Respondent to a contract. A response by a corporation shall further give the state of incorporation and whether the Respondent is qualified to do business in Rhode Island as a foreign corporation. A Response submitted by an agent shall have a current power of attorney attached certifying the agent’s authority to bind the Respondent.

1.15 PROPOSAL DOCUMENTS

1.15.1 One complete RFP may be obtained by interested parties, at no cost, from Customer.

1.15.2 Additional copies of the RFP may be secured at a cost of $5.00 to the Respondent upon request and payment to the issuing office designated in the Advertisement.

1.15.3 In making copies of the RFP available on the above terms, the Customer does so only for the purpose of obtaining Responses on the Work and does not confer a license or grant permission for any other use of the RFP.

1.16 PROCEDURES

1.16.1 FORM AND STYLE OF RESPONSES

1.17 CLARIFICATION

1.17.1 Each Respondent shall carefully examine all RFP documents and related materials, addenda or other revisions, to thoroughly familiarize themselves with all requirements prior to submitting a Proposal. Should a Respondent find discrepancies or ambiguities in, or omissions from the Proposal documents, or should the Respondent be in doubt as to their meaning, Respondent shall at once and in any event, not later than the deadline for submitting questions (see Invitation to Bid), submit to Customer a written request for interpretation or correction thereof.

1.17.2 All questions or clarifications must be submitted via email to Howard Allen, hallen@riconvention.com, or be delivered in writing to the submission address listed on the Invitation to Bid.

1.17.3 Oral inquiries will be accepted only for clarification of administrative questions regarding this RFP.

1.17.4 No inquiries will be accepted after the deadline.

1.17.5 Any interpretation or correction of the RFP will be made by written addenda to all Respondents. No allowance will be made after Proposals are received for oversight, omission, error, or mistake by the Respondent or Customer. Addenda so issued will become part of the Proposal Documents and receipt thereof by the Respondent shall be acknowledged in the Proposal.

1.18 MODIFICATION OR WITHDRAWAL OF RESPONSE

1.18.1 A Response may not be modified, withdrawn or cancelled by the Respondent during the time period following the date designated for the opening of the Responses, and each Respondent so agrees in submitting a Response.

1.18.2 Prior to the time and date designated for receipt of Responses, a Response submitted may be modified or withdrawn by notice of the party receiving Responses at the place designated for receipt of Responses. Such notice shall be in writing over the signature of the Respondent. A change shall be so worded as not to reveal the amount of the original Response.

1.18.3 Withdrawn Responses may be resubmitted up to the date and time designated for the receipt of Responses provided that they are then fully in conformance with these Instructions to Respondents.

1.19 DUE DILIGENCE

1.19.1 Prior to submitting a Proposal, each Respondent shall make all investigations and examinations necessary to ascertain conditions and requirements affecting operation of the proposed services. Failure to make such investigation and examinations shall not relieve the successful Respondent of the obligation to comply, in every detail, with all provisions and requirements, nor shall it be a basis for any claim whatsoever for alteration in any provision required by the Contract.

1.20 CONDITIONS AND LIMITATIONS

1.20.1 The Proposals and any information made a part of the Proposals will become part of SMG and RICCA's official files without any obligation on SMG and RICCA's part to return them to the individual Respondent(s).

1.20.2 This RFP and the selected Respondent(s) Proposal may, by reference, become a part of any formal Contract between SMG and Respondent resulting from this solicitation.

1.20.3 Respondent(s) shall not offer any guarantees, favors, or anything of monetary value to any official or employee of SMG, RICCA or the State of Rhode Island for the purposes of influencing consideration of a proposal.

1.21 CONSIDERATION OF RESPONSES

1.21.1 OPENING

1.21.1.1 The properly identified Responses received on time will be opened publicly and acknowledged.

1.21.1.2 To be considered for the award, a Respondent must be experienced and regularly in the business of providing the Scope of Work required by the RFP and must have a business phone and be available for consultation.

1.21.2 REJECTION OF RESPONSES

1.21.2.1 SMG shall have the right to reject any responses that propose equipment that has been banned or restricted by the Federal, State, or Local governments.

1.21.2.2 SMG shall have the right to reject any or all Responses, reject a Response not accompanied by the data required by the RFP, or reject a Response which is in any way incomplete or irregular.

1.21.3 ACCEPTANCE OF A RESPONSE

1.21.3.1 It is the intent of SMG to award a Contract to the qualified and responsive Respondent submitting the response which is in the best financial interest of SMG and RICCA, provided the Response has been submitted in accordance with the requirements of the RFP. SMG shall have the right to accept the Response which in SMG's judgment, is in the best interests of SMG and RICCA.

1.21.3.2 Following the evaluation of written proposals, Respondent(s) may be requested to offer oral presentation to SMG. Failure to comply with such a request will disqualify Respondent from consideration.

1.22 FORM OF AGREEMENT BETWEEN SMG AND RESPONDENT

1.22.1 The successful Respondent will be required to enter into a written Contract with SMG.

1.22.2 MINORITY BUSINESS ENTERPRISE

1.22.2.1.1 SMG may, after considering the financial impact to SMG and RICCA, prior to making a final determination of award, apply special consideration to the offer of Minority Business Enterprises in accordance with the Rhode Island General Laws and the applicable regulations.

1.22.2.1.2 A Minority Business Enterprise shall mean a small business concern owned and controlled by one or more minorities or women and is certified by the Rhode Island Department of Economic Development to meet the definition established by Rhode Island law.

1.23 EVALUATION CRITERIA

1.23.1 The successful Respondent shall be determined by the following criteria:

1.23.1.1 Respondents must demonstrate the ability to provide the Work specified by furnishing information regarding its expertise, experience, financial soundness and integrity.

1.23.1.2 Respondents and personnel must demonstrate an understanding of the Work required and be able to dedicate sufficient time to be able to complete the Work required.

1.23.1.3 Respondents must demonstrate that Jobs of similar scope and/or magnitude have been successfully maintained.

1.23.1.4 Responses will be evaluated on the basis of the above and the relative merits of the proposal, in addition to price.

1.23.1.5 SMG reserves the right to award the Contract on the basis of the initial Response.

1.24 GENERAL

1.24.1 USE OF FACILITIES

1.24.1.1 The Vendor’s employees must check-in and exit the Customer premises at the designated entrance only.

1.24.1.2 The Vendor’s truck and other vehicles must have the company name or logo permanently attached and must be parked in authorized areas or spaces only.

1.24.1.3 The Vendor shall take all precautions necessary and shall bear the sole responsibility for the safety of the Work, and the safety and adequacy of the methods and means it employs in performing Work. Vendor, while on the Center’s grounds must also observe any safety requirements imposed by SMG.

1.24.2 LENGTH OF CONTRACT

1.24.2.1 The Contract under which these privileges shall be granted will be for a term of up to three (3) years.

1.24.2.2 Vendor shall understand that legislation passed by the State of Rhode Island, during the Contract Term, to change or regulate prices may cause the parties hereto to re-negotiate or adapt the Agreement to the laws as they are written.

1.24.2.3 Customer shall reserve the right to terminate this contract at any time on thirty (30) days' notice, without penalty.

1.24.3 FAILURE TO COMPLETE WORK ON TIME

1.24.3.1 Delays in completion of Work will cause delay in use by the owner and will cause various losses to SMG, including revenue.

1.24.3.2 Respondents agree to pay an amount, agreed upon by both parties, for each and every calendar day they are in default in completing the Work. (Typically this amount is between $100 – 200 USD per business day for projects of this size).

1.24.4 BONDING

1.24.4.1 Vendor will be required to execute a Performance and Payment Bond, in a form acceptable to RICCA/SMG, in the amount of One Hundred Thousand Dollars ($100,000.00) with Corporate Surety to secure the performance by the Vendor of all terms of the Contract. The Performance and Payment Bond shall name SMG and RICCA as beneficiaries and be in place upon the execution of the Contract.

1.24.5 INSURANCE

1.24.5.1 During the contract term, the Vendor will maintain, at its sole cost and expense, policies written by an insurance company or companies approved by SMG, authorized and licensed to do business in the State of Rhode Island and rated not less than "A-" by the most current Best's Manual. All such insurance coverage, with the exception of Workers' Compensation, shall name SMG, the Center, RICCA, the State of Rhode Island and their employees, agents, officers and directors as additional insureds on a primary and non- contributing basis there under and a waiver of subrogation in favor of all additional insureds shall apply to all such coverage. Evidence of such coverage being in place will be promptly delivered to SMG prior to the Commencement of the Term. All such coverage shall be endorsed to indicate that coverage will not be materially changed or cancelled without at least thirty (30) days,' prior written notice to SMG, such prior notice being mandatory. The Vendor will provide SMG with evidence of the renewal of all coverage required for the Contract. Such coverage shall include the following:

1.24.5.1.1 Comprehensive General Liability coverage in the amount of $2,000,000 in the aggregate and $1,000,000.00 each occurrence. This coverage must be written on an occurrence form, claims made policies will be unacceptable. The Comprehensive Liability insurance shall cover the vendor, SMG, the Center, RICCA, the State of Rhode Island and their respective employees, agents, officers and directors from and against any claim arising out of personal injury and/or property damage as a result of the operations of the Vendor or its failure to comply with the terms and provisions of the Contract. Such policy or policies for the insurance shall include coverage for claims of any persons as a result of incidents directly or indirectly related to the employment of such persons by the Vendor or by any other persons. This coverage shall include blanket contractual insurance and such coverage shall make express reference to the indemnification provisions set forth in the Contract.

1.24.5.1.2 Worker’s Compensation Coverage, as statutorily required by the State of Rhode Island, for all employees of the Vendor. Employer’s Liability coverage on the Workers’ Compensation policy shall be written in the minimal amount of $1,000,000.00.

1.24.5.1.3 Excess Liability Coverage in the amount of $5,000,000.00 shall be in the form of an Umbrella policy rather than a following form excess policy. This policy or policies shall be specifically endorsed to be excess for the required Comprehensive General Liability Coverage, the Employees’ Liability Coverage on the Workers’ Compensation policy, and the Comprehensive Automobile policy.

1.24.5.1.4 Comprehensive Automobile Liability Coverage, in an amount not less than $1,000,000.00, shall be maintained. Such coverage will include all owned, non-owned, leased and/or hired motor vehicles, which may be used by the Vendor in connection with the services required under this Contract.

1.24.5.1.5 Insurance against Loss and/or Damage to fixtures, furnishings, equipment and other personal and business property of the Vendor and the Center upon the premises by fire or other such casualty as may be generally included in the usual form of extended coverage in an amount equal to the replacement costs of such property. Such insurance shall provide coverage for the personal property of others in the care, custody and control of the Vendor that is used by the Vendor for the Work.

1.24.6 INDEMNIFICATION

1.24.6.1 The Vendor hereby agrees to indemnify and keep indemnified, defend, hold and save harmless RICCA, SMG, the State of Rhode Island and their respective agents, representatives, consultants, directors, officers and employees from and against any and all actions, causes of action, claims, demands, liabilities, losses, penalties, judgments, awards, costs, damages or expenses of whatsoever kind and nature, including reasonable counsel or attorneys' fees and court costs, which RICCA, SMG, the State of Rhode Island and their respective agents, representatives, consultants, directors, officers and employees shall or may at any time sustain or incur, directly or indirectly, by reason of (a) any breach by the Vendor of any representation, warranty, covenant or agreement in the Contract, (b) any failure by the Vendor to perform its obligations under the Contract, (c) failure by the Vendor or its agents, employees, suppliers or subcontractors to observe and comply with all applicable federal, state and local laws, ordinances, rules and regulations, or (d) arising out of or resulting from the Work, provided that any such claim, damage, loss or expense with respect to the Work is (i) attributable to bodily injury, sickness, disease or death or to injury to or destruction of tangible property including the loss of use resulting there from, and (ii) caused in whole or in part by any negligent act or omission of the Vendor, any subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, regardless of whether or not it is caused in part by a party indemnified hereunder. By virtue of this indemnification clause, the Vendor does not waive any rights or defenses it may have with respect to any such claims, demands and causes of action, including the right of contribution.

1.24.6.2 In any and all claims against SMG, the State of Rhode Island, RICCA and their respective agents, representatives, consultants, directors, officers or employees by any employee of the Vendor any subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, the indemnification obligation under the previous paragraph shall not be limited in any way by any limitation on the amount of the type of damages, compensation or benefits payable by or for the Vendor or any subcontractor, the workers' or workmen's compensation acts, disability benefits acts or other employee benefit acts.

1.25 LABOR

1.25.1 Vendor shall provide, at its own expense, qualified or licensed labor in the applicable trades.

1.25.2 Employees shall be uniformly dressed, clean and neat in appearance. All employees must display identification prominently while on the Customer premises.

1.25.3 All employees shall be qualified and properly trained in the handling and use of all Equipment used in and around the Center.

1.25.4 RICCA has the right of approval of any and all Vendor employees.

1.25.5 SMG has the right to assign and adjust all work hours and schedules not to impact any Events at the Center.

1.25.6 Equal Employment Opportunity Compliance – The Vendor is required to demonstrate the same commitment to equal opportunity as prevails under federal contracts controlled by

Federal Executive Orders 11246, 11625 and 11375. Affirmative action plans shall be submitted by the Vendor to the RICCA, if required. Vendor's failure to abide by the rules, regulations, contract terms and compliance reporting provisions as established shall be grounds for forfeiture and penalties.

1.25.7 Prevailing Wage Requirement – In accordance with Title 37 Chapter 13 of the General Laws of Rhode Island, payment of the prevailing rate of per diem wages and general prevailing rate for regular, overtime and other working conditions existing in the locality for each craft, mechanic, teamster, or type of workmen needed to execute this Work is a requirement for both contractors and subcontractors for all public works. Vendor shall submit a true copy of completed payroll records for any work done relating to the Contract to SMG on a weekly basis.

1.25.8 Drug-Free Workplace Requirement – In Accordance with Executive Order No. 91- 14, Vendor shall abide by Rhode Island's drug-free workplace policy and the Vendor shall so attest by signing a certificate of compliance.

1.26 PERMITS, LICENSES AND LAWS

1.26.1 Vendor shall be required to provide and maintain any permits and licenses required by law at its own expense. A set of blueprints will be provided if needed.

1.26.2 Vendor shall at all times observe and comply with all applicable federal, state and local laws, ordinances, rules and regulations, and shall indemnify, save and hold harmless, the RICCA and SMG and all of their officers, agents and employees against all claims or liability arising from or in connection with the violation of any such law, ordinance, rule or regulation, whether such violation is caused by Vendor, or its agents, employees, suppliers, or subcontractors.

1.27 STANDARDS OF DESIGN AND WORKMANSHIP

1.27.1 All aspects of the maintenance work shall be designed, tested, implemented, and documented in accordance with recognized professional and industry practices. All work shall be performed by qualified technicians.

1.28 INSTALLATION

1.28.1 The contractor shall furnish all equipment, accessories, and material required for the proper installation and operation of all systems in compliance with these specifications and applicable contract drawings. Any material and/or equipment necessary for the proper function and operation of the systems, which is not specified or described herein, shall be deemed part of this specification, unless noted as provided by others.

1.1 MANUFACTURER SUBSTITUTION POLICY

1.1.1 Customer has in some cases specified specific manufacturers or models (e.g., Axis camera products). Requests for exception to the preferred products listed may be submitted in writing to the customer no later than one (1) week prior to bid submittals. Such requests shall include all engineering documentation, drawings, third party test reports proving equivalency in transmission characteristics, mechanical features, and end to end solution performance. Acceptance of equivalent products shall be in written form by the customer to be valid. Approved products substituted for those listed in this document without written prior approval from the customer shall be removed and replaced at the contractor's expense.

1.2 PROPRIETARY INFORMATION

1.2.1 Customer shall retain ownership of all proprietary information, and disclosure of information does not convey any right or license to use the information other than for the stated purpose.

1.3 VENDOR ACTIVITIES

1.3.1 Vendor’s activities are not to be disruptive of normal business activity–including excessive construction noises– and must not compromise the safety, security or self-respect of any of the Customer's employees or visitors in any way. The Customer reserves the right to insist that any individual under the direction of the vendor may, without a statement of cause, be taken off this project. The vendor will comply without compromising schedules or other contract terms.

1.4 DUE CARE

1.4.1 In delivering, installing and removing equipment, due care shall be exercised to avoid damage to, or disfigurement of, buildings, equipment, driveways or other property. Any blemish made by Vendor to the physical plant or property of Customer is to be restored by the Vendor. The successful vendor shall be required to complete restorations at its expense for any damage caused by it or by any of the subcontractors.

1.5 RUBBISH

1.5.1 The Contractor shall maintain the premises free from rubbish caused by his work, employees, or sub-contractors, by removing it as specified in the bid or when directed by the Customer. At the completion of his work, he must remove all surplus materials and rubbish from the premises to the satisfaction of the Customer.

1.6 OBSOLETE EQUIPMENT AND CABLE

1.6.1 Contractor shall demolish, remove from the job site, and dispose of all equipment and cable that is being replaced and/or made obsolete by the work under this project. Contractor shall provide Customer a list of all equipment and materials to be removed, and Customer must approve this list prior to demolition or removal.

1.6.2 Equipment slated for disposal must first be cleared of customer specific information and data, and memory / storage devices wiped or destroyed.

1.7 PERFORMANCE REQUIREMENTS

1.7.1 All systems and equipment shall be certified to meet the following standards:

1.7.1.1 ISO 9000

1.7.1.2 System shall be RoHS (Restriction of Hazardous Substances) compliant and meet proposed amendments to the reduction of toxic substances in manufacturing as stated in the Environmental Design of Electrical Equipment Act (EDEE)

1.7.1.3 Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency and marked for intended location and application

1.7.1.4 Installation shall comply with NECA 1-2010 “Standard Practice of Good Workmanship in Electrical Construction”

1.7.1.5 Installation shall comply with NEC/NFPA 70E “Standard for Electrical Safety in the Workplace”

1.7.1.6 Installation shall comply with FCC CFR 47 Part 15 Class A "Telecommunications, Radio Frequency, Digital Device Emission”

1.7.1.7 Installation shall comply with federal, state, and local codes and Authority Having Jurisdiction (AHJ)

1.8 ACTION SUBMITTALS

1.8.1 Product Data: Provide details and technical specifications for each product indicated. Include physical dimensions, features, performance, electrical characteristics, ratings, software versions, and operating system details.

1.8.2 Shop Drawings: Include system line diagrams, equipment locations, installation details, and system integration plans.

1.8.2.1 Detail equipment assemblies and indicate dimensions, weights, loads, required clearances, method of field assembly, components, and location and size of each field connection.

1.8.2.2 Functional Block Diagram: Show single-line interconnections between components for signal transmission and control. Show cable types, quantities, and sizes.

1.8.2.3 Plans and Elevations: Dimensioned plans and elevations of equipment racks, enclosures, and conduit interconnections, including access and workspace requirements.

1.8.2.4 Wiring Diagrams: For power and signal wiring.

1.8.3 Equipment and Software List: Include every piece of equipment and software by product/model name and/or number, manufacturer, serial number, revision number, location, and date of original installation. If factory and/or bench testing regimens are required by the project plan, add pretesting record of each piece of equipment and software, listing name of person testing, date of test, and adjustments made.

1.8.4 The Proposer shall also deliver original copies of all licenses, registrations, documentation, disks and other media as may have been included with those commercially available software packages provided with the system. In addition, the Proposer shall ensure that all licenses, registrations and warranties have been transferred prior to final system turnover.

1.9 INFORMATIONAL SUBMITTALS

1.9.1 ISO9000 Listing Certificates

1.9.2 CE and FCC Compliance Certificates:

1.9.3 Field quality-control reports

1.9.4 Current Integrator Certification Letter

1.9.5 Current Training Certificates (listing expiration dates) for **<two (2)>** technicians from the supporting office

1.9.6 Warranty: Software support and warranty information for all components, including Service Level Agreement (SLA) details, and duration of agreement from date of system acceptance by Owner

1.10 CLOSEOUT SUBMITTALS

1.10.1 Operation and Maintenance Data: For all components and software to include in emergency, operation, and maintenance manuals.

1.10.1.1 Extra Materials: Return all left-over (unused) product and materials to the Owner

1.10.1.2 Applicable operating system, database, client, and application software on portable storage media

1.10.1.3 Full System Backup as of closeout date on portable storage media

1.10.1.4 Submit one (1) printed and one (1) electronic copy of project binder in final form. This copy shall contain as a minimum:

1.10.1.4.1 Table of Contents for each element

1.10.1.4.2 Contractor information - names phone numbers, and email for sales, technical support, and consumables reordering

1.10.1.4.3 Lists of spare parts and replacement components recommended to be stored at the site for ready access

1.10.1.4.4 Datasheets for all equipment

1.10.1.4.5 Operation and maintenance manuals for all equipment

1.10.1.4.6 Operation and maintenance procedures not covered in manufacture's manuals

1.10.1.4.7 Training:

1.10.1.4.7.1 Program Syllabus.

1.10.1.4.7.2 Manual(s) and Material(s).

1.11 QUALITY ASSURANCE

1.11.1 Installation shall comply with federal, state, and local codes and Authority Having Jurisdiction (AHJ)

1.11.2 Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

1.11.3 All software and hardware shall be programmed and installed in accordance with manufacturer's specifications.

1.11.4 All equipment shall be new, in current production, and the standard products of a manufacturer of ESS equipment.

1.11.5 Manufacturer shall guarantee availability of parts, for a minimum of **seven (7)** years from date of shipment.

1.11.6 On-site maintenance and repair service shall be available locally and within **four (4) hours** of notification of condition.

1.11.7 Contractor shall review drawings and specifications

1.11.8 Software integration between all integrated systems shall be tested and certified for interoperability by the manufacturer of each system.

1.12 PERMITS

1.12.1 All permits required for the specified performance and completion of the work shall be secured by the Contractor

1.13 PROJECT CONDITIONS

1.13.1 Environmental Conditions: System components shall withstand the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1.13.1.1 Interior Environmentally Controlled Space: Rated for continuous operation in ambient temperatures of 32° to 95° F (0° to 35° C) dry bulb and a relative humidity of 20 to 80 percent, noncondensing.

2 ESS Systems

2.1 GENERAL SCOPE

2.1.1 RICC recognizes that its existing Electronic Security Systems (ESS) are approaching end-of-life product availability and technical support status and will not support expansion to include the Garrahy Garage.

2.1.2 RICC recognizes the need for an enterprise level unified security system, and intends to engage a system integrator that can install and support an enterprise level security system.

2.1.3 The following security systems shall be integrated into the overall Electronic Security System (ESS). The technologies that will comprise ESS include:

2.1.3.1.1 Video Surveillance System (VSS)
2.1.3.1.2 Access Control (ACS)

2.1.4 The Garrahy Courthouse Parking Structure is expected to add the need for:

- 10 Doors of access control and/or monitoring
  - 5 shall connect to the new garage access control system
  - 5 shall connect to the existing courthouse access control system
- 56 Surveillance Cameras
  - 56 shall connect to the new garage video management system,
    - 15 of the 56 shall also stream to the existing courthouse video management system
  - Model Breakdown:
    - AXIS P3245-LVE (qty -23)
    - AXIS P3807-PVE (qty -1)
    - AXIS Q1786-LE (qty -4)
    - AXIS Q3517-LVE (qty -28)
  - Accessories:
    - AXIS T91B51 Ceiling Mount (qty -31)
    - AXIS T91B52 Extension Pipe 100 cm (qty -19)
    - AXIS T91D61 Wall Mount 1.5” NPS (qty -10)
    - AXIS T91H61 Wall Mount (qty -4)
    - AXIS T94M01D Pendant Kit (qty -26)
    - AXIS T94T01D Pendant Kit (qty -19)

2.1.5 System Storage shall be sized to support:

2.1.5.1 Continuous, full resolution recording for all cameras,

2.1.5.2 Retain Minimum 30 days

2.1.5.3 15 FPS

2.1.5.4 Plus an additional 25% for future growth

2.1.6 Cameras shall be installed as shown on the attached line diagrams and drawings, and situated to observe all perimeter entrances and exits, as well as key interior areas.

2.1.7 Locking hardware (door strikes) will be provided by the general contractor as part of the door installation.

2.1.8 Garage cameras shall also be situated to observe lane transition and traffic at key points throughout the facility as determined by management.

2.1.9 Cameras shall be placed to view activity in elevator cabs and elevator lobbies.

2.1.10 All cameras shall stream to the new system, and selected cameras (first and lower levels) shall also stream to the Capitol Police VSS.

2.1.11 The ACS will have automated interconnectivity and cross-functionality with the VSS. Predetermined alarms and events detected by the Access Control System shall trigger automatic reactions in the Video Surveillance System and vise-versa. This integrated functionality will enhance security operator efficiency and effectiveness.

2.1.12 All alarms will be recorded and annunciated in the RICC Security Operations Center (SCC) and/or other locations designated by the owner.

2.1.13 Surveillance system’s video recorders and associated video control head-end equipment will be rack-mounted within the Security Equipment Room.

2.1.14 The badges will be printable 13.56 MHz proximity PVC cards with vertical slot punched for a badge strap. The badge card number will use a registered 48-bit format.

2.1.15 The access control Intelligent Field Panels (IFP) will be microprocessor-controlled units. The panels will serve as the data collection and communications interface between the host and the field devices, such as card readers, alarm inputs and control outputs. The IFPs will be located in secure locations such as IT closets and security equipment rooms. The IFPs will employ a distributed processing methodology, so as to function independently of the head-end database and software.

2.1.16 The selected integrator shall be responsible for conduits and pathways for the Electronic Security System (ESS). See section entitled “Cabling and Pathways”.

2.1.17 All components will interface with each other. For example, alarm activation or invalid ACS transactions will cause VSS cameras to pan, tilt and zoom (PTZ), and display the covered area camera image onto a designated monitor screen, and start the recording equipment to record in a real time mode.

3 Video Management System

3.1 VMS GENERAL REQUIREMENTS

3.1.1 Surveillance system's video recorders and associated video control head-end equipment will be rack-mounted within the Security Equipment Room. Monitors will be located within the Security Operations Center; the monitor placement will be designed consistent with operational requirements. The monitors will be a console and wall mounted configuration. Remote monitors located at the building security desk, at the main entry of the emergency department, will be built into the casework.

3.1.2 The VMS shall be based on a true open architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage.

3.1.3 The VMS shall offer a complete and scalable video surveillance solution that shall allow cameras to be added on a unit-by-unit basis.

3.1.4 The VMS shall interface with analog-to-digital video encoders and IP cameras

3.1.5 The VMS shall integrate DVS using the DVS native SDK or using the following industry standards to interface to the DVS: ONVIF

3.1.6 All video streams supplied from analog cameras or IP cameras shall be digitally encoded in H.265, or H.264.

3.1.7 Each camera's bit rate, frame rate, and resolution shall be set independently from other cameras in the system, and altering these settings shall not affect the recording and display settings of other cameras.

3.1.8 The VMS shall be able to use multiple CCTV keyboards to operate the entire set of cameras throughout the system, including brands of cameras from various manufacturers and including their PTZ functionalities (i.e.: Pelco keyboard controls Panasonic dome or vice-versa).

3.1.9 The VMS shall be able to retrieve and set the current position of PTZ cameras using XYZ coordinates.

3.1.10 The VMS shall support PTZ camera protocols from multiple manufacturers, including analog and IP protocols.

3.1.11 The VMS shall arbitrate the user conflict on PTZ usage based on user levels per camera.

3.1.12 The VMS shall support the following list of CCTV keyboard protocols:

3.1.12.1 American Dynamics 2078 ASCII, and American Dynamics 2088 ASCII

3.1.12.2 Bosch Autodome, Bosch Intuikey

3.1.12.3 DVTel

3.1.12.4 GE ImpactNet

3.1.12.5 Panasonic, Pelco ASCII, Pelco KBD-300, and Pelco P.

3.1.12.6 Radionics

3.1.12.7 Samsung SSC-1000 and SPC-600

3.1.12.8 Videoalarm

3.1.12.9 Sony RM-NS1000

3.1.12.10 Panasonic WV-CU161C

3.1.13 The VMS shall support the following list of joysticks and control keyboards:

3.1.13.1 Axis 295.

3.1.13.2 Axis T8310 Video Surveillance Control Board.

3.1.13.3 Panasonic WV-CU950 Ethernet keyboard.

3.1.13.4 Any USB joystick detected as a Windows Game Controller.

3.1.14 The VMS shall allow for the configuration of a time zone for each camera connected to a DVS. For playback review, users shall have the ability to search for video based on the following options:

3.1.14.1 Local time of the camera

3.1.14.2 Local time of the SSM

3.1.14.3 Local time of user’s workstation

3.1.14.4 GMT Time

3.1.15 Audio and Video storage configuration for the SSM shall either be:

3.1.15.1 Internal or external IDE/SATA/SAS organized or not in a RAID configuration.

3.1.15.2 Internal or external SCSI/iSCSI/Fiber Channel organized or not in a RAID configuration.

3.1.15.3 Within the overall storage system, it shall be possible to include disks located on:

3.1.15.3.1 External PCs on a LAN or WAN

3.1.15.3.2 Network Attached Servers (NAS) on a LAN or WAN

3.1.15.3.3 Storage Area Networks (SAN)

3.1.15.3.4 The SSM shall not limit the actual storage capacity configured per server.

3.2 CYBER SECURITY REQUIREMENTS

3.2.1 The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.

3.2.2 The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:

3.2.3 ADFS (Active Directory Federation Services)

3.2.4 The USP shall limit the IP ports in use and shall provide the Administrator with the ability to configure these ports.

3.2.5 The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate based authentication leveraging RTSPS (RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.

3.2.6 The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate based AES 128-bits encryption. The VMS shall:

3.2.6.1 Allow encryption to be set on a per camera basis for all or some of the cameras.

3.2.6.2 Provide up to 20 different certificates for different groups of CSA or users who have been granted access to decrypted streams.

3.2.6.3 Not decrease the recording performance by more than 50% when encryption is enabled.

3.2.6.4 Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.

3.2.6.5 Use a random encryption key and change periodically.

3.2.6.6 Allow encrypted streams to be exported.

3.2.7 The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.

3.3 ARCHIVING

3.3.1 The Archiver (role) shall use an event and timestamp database for the advanced search of audio/video archives. This database shall use Microsoft SQL.

3.3.2 The Archiver shall protect archived audio/video files and the system database against network access and non-administrative user access.

3.3.3 The Archiver shall digitally sign recorded video using 248-bit RSA public/private key cryptography.

3.4 CLOUD ARCHIVING

3.4.1 The VMS shall support the automatic transfer of video recorded on the Archiver to the cloud, based on the age of the video.

3.4.2 The Archiver shall encrypt recordings using AES-256 prior to transferring video to the cloud and maintain encryption keys local to the user's system.

3.4.3 The VMS shall support TLS encryption between the on-premises Archiver and the cloud.

3.4.4 The VMS shall allow users to search video stored in the cloud through the same functionality used when querying video that is stored locally.

3.4.5 The VMS will maintain a local cache of video downloaded from the cloud, in order to playback recordings without requiring an additional transfer.

3.5 VMS ANALYTICS

3.5.1 The analytics shall automatically detect the intrusion of persons or vehicles in critical areas.

3.5.2 The analytics shall be completely unified with the Video Management System.

3.5.3 Configuration shall natively be performed in the configuration interface of the Video Management System.

3.5.4 The analytics shall feature rain and haze filters to filter out disturbances.

3.5.5 The analytics shall feature two different detection variants:

3.5.6 Trigger an alarm if a motion pattern moves from zone A (source) through zone B into zone C (sink).

3.5.7 Trigger an alarm if a motion pattern moves anywhere inside a specified zone.

3.5.8 The analytics shall support an unlimited number of detection areas (each with its own zones and settings).

3.5.9 The analytics shall employ feature-point-based tracking algorithms to detect and analyze motion.

3.5.10 The analytics shall not employ pixel-based object tracking but shall employ grid- based analysis (using cues at multiple scales for analytics).

3.5.11 The analytics shall offer the possibility to configure object movement paths.

3.5.12 The analytics shall not employ tripwires or cross-lines.

3.5.13 Areas and the scenes perspective (near & far object size) shall be configured on- screen using a point-and-click interface.

3.5.14 The analytics shall feature filters for movement speed, distance, and direction to detect events.

3.5.15 The analytics shall be fully server-based, with no calculation on cameras necessary.

3.5.16 The analytics shall operate with color, thermal, and infrared cameras.

3.6 PRIVACY PROTECTION

3.6.1 System shall provide privacy protection, including but not limited to the following capabilities:

3.6.1.1 Automatically obscure all movement in surveillance videos in real-time.

3.6.1.2 Provide live privacy masking of moving objects (such as people and vehicles).

3.6.1.3 Masks movements using blocks, thus obscuring the outline of an object or person.

3.6.1.4 Scrambling methods to include: Average, Average Ghost, Colorize, Colorize Difference, Colorize Ghost, Icon, Image, and Blur.

3.6.2 Privacy features shall be completely unified with and configured via the video management system. No calculation on the camera should be needed.

3.6.3 Masking grids shall be configurable via a point-and-click interface.

3.6.4 Analysis resolution should be adjustable to optimize performance.

3.7 GENERAL CLIENT SOFTWARE REQUIREMENTS

3.7.1 The Client Software Applications (CSA) shall provide the user interface for USP configuration and monitoring over any network and be accessible locally or from a remote connection.

3.7.2 The CSA shall consist of the Configuration UI for system configuration and the Monitoring UI for monitoring. The CSA shall be Windows-based and provide an easy-to-use graphical user interface (UI).

3.7.3 The CSA for monitoring shall support running in 64-bit mode.

3.7.4 The Server Administrator shall be used to configure the server database(s). It shall be web-based and accessible locally on the SSM or across the network.

3.7.5 The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and the .NET software framework.

3.7.6 All applications shall provide an authentication mechanism, which verifies the validity of the user. As such, the administrator (who has all rights and privileges) can define specific access rights and privileges for each user in the system.

3.7.7 When integrated with Microsoft's Active Directory, the CSA and USP shall authenticate users using their Windows credentials.

3.7.7.1 An operator shall be able to launch a specific task only if he or she has the appropriate privileges.

3.7.7.2 The Home Page content shall be customizable through the use of privileges to hide tasks that an operator should not have access to and through a list of favorite and recently used tasks. In addition, editing a USP XML file to add new tasks on the fly shall also be possible.

3.7.8 The Contractor shall provide up to 5 simultaneous Clients.

3.8 CONFIGURATION USER INTERFACE (UI)

3.8.1 The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration. The Configuration UI shall provide decentralized configuration and administration of the USP system from anywhere on the IP network.

3.8.2 The Configuration UI shall provide the ability to change video quality, bandwidth, and frame rate parameters on a per camera (stream) basis for both live and recorded video.

3.8.3 The Configuration UI shall provide the ability to change video quality by a selection of predefined video quality template.

3.8.4 The Configuration UI shall provide the ability to configure brightness, contrast, and hue settings for each camera on the same DVS.

3.8.5 The Configuration UI shall provide the capability to enable audio recording on DVS units that support audio.

3.8.6 The Configuration UI shall provide the ability to change the audio parameters, serial port and I/O configuration of individual DVS units.

3.8.7 The Configuration UI shall provide the capability to rename all DVS units based on system topology and to add descriptive information to each DVS.

3.8.8 The Configuration UI shall provide the ability to set recording schedules and modes for each individual camera. The recording mode can be:

3.8.8.1 Continuous.

3.8.8.2 On motion and Manual.

3.8.8.3 Manual only.

3.8.8.4 Disabled.

3.8.9 The Configuration UI shall support the creation of schedules to which any of the following functional aspects can be attached:

3.8.9.1 Video quality (for each video stream per camera).

3.8.9.2 Recording (for each camera).

3.8.9.3 Motion detection (for each detection zone per camera).

3.8.9.4 Brightness, Contrast, and Hue (for each camera)

3.8.9.5 Camera sequence execution

3.8.10 The Configuration UI shall support the creation of unlimited recording schedules and the assigning of any camera to any schedule.

3.8.11 The Configuration UI shall detect and warn user of any conflict within assigned schedules.

3.9 VMS CLIENT USER INTERFACE (UI)

3.9.1 The Monitoring UI shall fulfill the role of a Unified Security Interface that is able to monitor video, and access control events and alarms, as well as view live and recorded video.

3.9.2 The Monitoring UI shall provide a graphical user interface to control and monitor the USP over any IP network. It shall allow administrators and operators with appropriate privileges to monitor their unified security platform, run reports, and manage alarms.

3.9.3 Dynamically Adaptive UI, Dashboard, and Widgets

3.9.3.1 The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.

3.9.3.2 Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions.

3.10 SERVER ADMINISTRATOR USER INTERFACE REQUIREMENTS

3.10.1 The Server Administrator shall be used to configure the SSM and the Directory Role (main configuration) and its database(s), to apply the license, and more.

3.10.2 The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.

3.10.3 Access to the Server Administrator shall be protected via login name, password, and encrypted communications.

3.10.4 The Server Administrator shall allow the administrator (user) to perform the following functions:

3.10.4.1 Manage the system license.

3.10.4.2 Configure the database(s) and database server for the Directory Role,

3.10.4.3 Activate/Deactivate the Directory Role.

3.10.4.4 Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.

3.10.4.5 Define the client-to-server communications security settings.

3.10.4.6 Configure the network communications hardware, including connection addresses and ports.

3.10.4.7 Configure system SMTP settings (mail server and port).

3.10.4.8 Configure event and alarm history storage options.

3.11 UNIFIED WEB CLIENT (UWC) GENERAL REQUIREMENTS

3.11.1 The USP shall support a unified web client (UWC) for access control and video.

3.11.2 The UWC shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.

3.11.3 The UWC shall be platform independent and run within Microsoft Edge, Internet Explorer, Firefox, Safari, and Google Chrome.

3.12 SMARTPHONE AND TABLET APP GENERAL REQUIREMENTS

3.12.1 The USP shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the USP over any WiFi or mobile network connection.

3.12.2 Mobile apps shall communicate with the USP via a Mobile Server (same as the Unified Web Client or UWC). Communication between the mobile device and the Mobile Server shall support optional encryption.

3.12.3 Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):

3.12.3.1 Apple iPod Touch, iPhone, and iPad.

3.12.3.2 Android-compatible smartphones and tablets.

3.12.4 It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play, Windows Store).

3.12.5 Functionalities

3.12.5.1 Live monitoring and command and control of the USP.

3.12.5.2 Receive alarm push notifications from the Apple Push Notification Server or from the Google Android push server.

3.12.5.3 Alarm management (view and acknowledge alarms, video tied to alarms).

3.12.5.4 View USP hierarchy and search for entities.

3.12.5.5 Stream video from the mobile device using the built-in camera.

3.12.5.6 Video streams from mobile devices shall be available in the USP to be viewed in live and recorded on the Archiver.

3.12.6 Video

3.12.6.1 View live and playback video at 320 x 240, 640 x 480 or 1280 x 1024 @ 15 fps.

3.12.6.2 Monitor camera status.

3.12.6.3 View up to 6 video feeds.

3.12.6.4 Control PTZ functionality of a camera, including access to PTZ presets.

3.12.6.5 Save snapshots locally on the device.

3.12.6.6 View video tied to access control events, and alarms.

3.13 HEALTH MONITOR

3.13.1 The USP shall monitor the health of the system, log health-related events, and calculate statistics.

3.13.2 USP services, roles, agents, units, and client apps will trigger health events.

3.13.3 The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.

3.13.4 A dedicated role, the Health Monitoring Role, shall perform the following actions:

3.13.4.1 Monitor the health of the entire system and log events.

3.13.4.2 Calculate statistics within a specified time frame (hours, days, months).

3.13.4.3 Calculates availability for clients, servers and video/access/ALPR units.

3.13.5 A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.

3.13.6 A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.

3.13.7 Detailed system care statistics will be available through a web-based dashboard providing health metrics of USP entities and roles, including Uptime and mean-time-between-failures.

3.13.8 Health events shall be accessible via the SDK (can be used to create SNMP traps).

3.14 USP GENERAL REQUIREMENTS

3.14.1 The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.

3.14.2 The USP shall support the seamless unification of IP access control system (ACS), IP video management system (VMS), and IP automatic license plate recognition system (ALPR) under a single platform. The USP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, and reporting of embedded ACS, VMS, and ALPR systems and associated edge devices.

3.14.3 Hardware and Software Requirements

3.14.3.1 The USP and embedded systems (video, license plate recognition, and access control) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.

3.14.3.2 The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.

3.14.3.3 The USP database server(s) shall be built on Microsoft's SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.

3.14.3.4 The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.

3.14.4 USP Access Control and Video - The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ACS, VMS, and ALPR. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.

3.14.5 USP Reporting - The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.

3.14.6 USP User and User Group Security, Partitions, and Privileges Management - The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if he or she has the appropriate privileges.

3.14.7 USP Event/Action Management - The USP shall support the configuration and management of events for video and ALPR. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.

3.14.8 USP Schedules and Scheduled Tasks - The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if he or she has the appropriate privileges.

3.14.9 USP Macros and Custom Scripts - The USP shall enable users to automate and extend the functionalities of the system through the use of macros or custom scripts for access control, video, and ALPR.

3.14.10 USP Dynamic Graphical Maps (DGM) - The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications, and shall provide a map centric interface with the ability to command and control all the USP capabilities from a full screen map interface.

3.14.11 USP Audit and User Activity Trails (Logs) -

3.14.11.1 The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

3.14.11.2 Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.

3.14.12 USP Incident Reports - Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.

4 Access Control Software and Database Management

4.1 ELECTRONIC ACCESS CONTROL SYSTEM GENERAL REQUIREMENTS

4.1.1 The ACS shall be an enterprise class IP access control software solution. It shall be fully embedded within a Unified Security Platform (USP). The USP shall allow the seamless unification of the ACS with an IP video management system (VMS).

4.1.2 The ACS shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.

4.1.3 The ACS shall support a variety of access control functionalities, including but not limited to:

4.1.3.1 Controller (Unit) management, door management, elevator management, and area management.

4.1.3.2 Cardholder and cardholder group management, credential management, and access rule management.

4.1.3.3 Badge printing and template creation.

4.1.3.4 People counting, area presence tracking, and mustering.

4.1.3.5 Offering a framework for third party hardware integration such as card and signature scanner.

4.1.4 The badges will be printable 13.56 MHz proximity PVC cards with vertical slot punched for a badge strap. The badge card number will use a registered 48-bit format.

4.1.5 The access control Intelligent Field Panels (IFP) will be microprocessor-controlled units. The panels will serve as the data collection and communications interface between the host and the field devices, such as card readers, alarm inputs and control outputs. The IFPs will be located in secure locations such as IT closets and security equipment rooms. The IFPs will employ a distributed processing methodology, so as to function independently of the head-end database and software.

4.1.6 Certification

4.1.6.1 The ACS shall be certified

4.1.6.1.1 UL-294

4.1.6.1.2 ULC-S319

4.1.6.1.3 EN-60839-11-1

4.2 ACS ACCESS MANAGEMENT

4.2.1 The ACS shall be based on an open architecture able to support multiple access control hardware manufacturers. The ACS shall be able to integrate with multiple non-proprietary interface modules and controllers, access readers, and other third-party applications.

4.2.2 The ACS shall be an IP enabled solution. All communication between the ACS and hardware controllers shall be based on standard TCP/IP protocol.

4.2.3 Access Manager Role

4.2.3.1 The Access Manager Role shall be the server that synchronizes all access control hardware units under its control, such as door controllers and I/O modules. It shall also be able to validate and log all access activities and events when the door controllers and I/O modules are online.

4.2.3.2 The Access Manager Role shall maintain the communication link with the hardware controllers under its control. It shall also continuously monitor whether the controllers are online or offline.

4.2.3.3 The Access Manager Role shall support doors and controllers located within one or more facilities. The Access Server shall support a minimum of 200 readers and up to 2000 readers per computer.

4.2.4 Synchronization of hardware units shall be automated and transparent to users and shall occur in the background. It shall also be possible to manually synchronize units or to synchronize units on a schedule.

4.2.5 The Access Server shall store all access events associated with the doors, areas, hardware zones (hardware input points), elevators, and controllers under its direct control.

4.3 ACS HARDWARE COMPATIBILITY LIST

4.3.1 The ACS shall have an open architecture that supports the integration of third-party IP-based door controllers and I/O modules. The ACS shall simultaneously support mixed configurations of access control hardware from multiple vendors.

4.3.2 The ACS shall support multiple types of hardware devices: single-reader controllers, 2-reader controllers, 1- to 64-reader controllers, integrated readers and door controllers, and Power-over-Ethernet (PoE) enabled door controllers.

4.3.3 The ACS shall support most industry standard card readers that output card data using the Wiegand protocol and Clock-and-Data.

4.3.4 The ACS shall support IP-enabled Mercury open source controllers and SIO modules

4.3.5 Where possible, field panels, power supplies and associated equipment will be located within secure IT closets.

4.3.6 The access control Intelligent Field Panels (IFP) will employ a distributed processing methodology, so as to function independently of the head-end database and software.

4.4 SEAMLESS UNIFICATION WITH VMS

4.4.1 Through the USP, the ACS shall support integration with an IP Video Surveillance System or MVS. Integration with an IP video surveillance system shall permit the user to view live and recorded video.

4.4.2 Users shall be able to associate one or more video cameras to the following entity types: doors, elevator, and hardware zone (input points) and more.

4.4.3 The Monitoring UI shall present a true Unified Security Interface for access control and video surveillance. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.

4.4.4 It shall be possible to view video associated with access control events when viewing a report.

4.5 ACS CONTROLLER (UNIT) MANAGEMENT

4.5.1 The ACS shall support the discovery, configuration, and management of IP enabled controllers and I/O modules (hardware units). A user shall be permitted to add, delete, or modify a controller if he or she has the appropriate privileges.

4.5.2 The ACS shall support automatic unit discovery. The user shall establish the settings for discovery ports and for the types of unit discovery and the ACS shall automatically detect all connected devices.

4.5.3 The ACS shall support a unit swap utility for swapping out an existing controller with a new controller. The unit swap utility shall avoid the reprogramming of the system whenever a unit is replaced. All logs and events from the old unit shall be maintained.

4.5.4 The ACS shall support pre-configuration of the system prior to the physical hardware installation.

4.5.5 The ACS shall support Firmware upgrade in bulk from the application.

4.6 ACS CARDHOLDER AND CARDHOLDER GROUP MANAGEMENT

4.6.1 The ACS shall support the configuration and management of cardholders and cardholder groups. A user shall be able to add, delete, or modify a cardholder or cardholder group if he or she has the appropriate privileges.

Custom fields shall be supported for both cardholders and cardholder groups.

4.7 ACS CREDENTIAL MANAGEMENT

4.7.1 The ACS shall support the configuration and management of credentials, e.g. access cards and keypad PIN numbers. A user shall be able to add, delete, or modify a credential if the user has the appropriate privileges.

4.7.2 Users shall be able to add Custom Fields (user-defined fields) to credentials. Creating a new credential shall be accomplished either manually or automatically.

4.7.3 Automatic creation shall allow the user to create a credential entity by presenting a credential to a selected reader. The ACS shall read the card data and associate it to the credential entity. It shall be possible to automatically enroll any card format (128 bits or less).

4.7.4 The ACS shall support multiple credentials per cardholder without necessitating duplicate cardholder information. The ACS shall automatically detect and prevent attempts to register an already-registered credential.

4.7.5 Batch enrollment of credentials shall be supported.

4.7.6 The ACS shall provide a workflow for badge issuance and card requests.

4.7.7 The ACS shall support the use of license plates as a credential.

4.7.8 The ACS shall natively support the creation and management of mobile IDs in the same way as other credentials.

4.8 ACS CUSTOM CARD FORMATS

4.8.1 A custom card format feature shall allow the administrator to add additional custom card formats using an intuitive tool within the Configuration UI. The custom card format tool shall be flexible in the following ways:

4.8.1.1 Once enrolled, new custom card formats shall appear in the card format lists for manual card enrollment.

4.8.1.2 An unrestricted number of additional custom card formats can be added.

4.8.1.3 Shall support credential with up to 256 bits.

4.8.1.4 The administrator shall be able to set the following options when defining a new format:

4.8.1.4.1 The order in which card fields appear in the user interface or CSA.

4.8.1.4.2 Whether a field is hidden from or visible to an operator.

4.8.1.4.3 Whether a field is read only or modifiable by an operator.

4.8.1.4.4 Complex parity checking schemes.

4.8.1.4.5 The order and location of a field’s data. Location can be defined on a bit-by- bit basis.

4.9 ACS BADGE DESIGNER

4.9.1 The badge designer shall allow the creation of badge templates that define the content and presentation format of a cardholder badge to be printed.

4.9.2 Badge production shall consist of selecting the credential, the badge template, and clicking print.

4.9.3 Batch printing of cards shall be available.

4.9.4 The contents of a badge template can include: cardholder’s first and last name, picture, custom fields, bitmap graphics, lines, ovals, rectangles, dynamic text labels linked to custom fields and static text labels, and barcodes (Interleaved 2 of 5, Extended Code 39).

4.9.5 Copy and paste of badge template objects shall be available.

4.9.6 It shall be possible to set the border thickness, and color, the fill color of badge objects (content), and the color of text labels.

4.9.7 Settings, such as object transparency, text orientation, and auto-sizing of text shall be available or transparent to the user.

4.9.8 Supported badge formats shall be (portrait and landscape): CR70 (2.875" x 2.125"), CR80 (3.37" x 2.125"), CR90 (3.63" x 2.37"), CR100 (3.88" x 2.63"), and custom card sizes.

4.9.9 Dual-sided badges shall be supported.

4.9.10 A badge template import and export function shall be available to allow the sharing of badge templates between distinct or independent ACS.

4.9.11 Chromakey shall be supported.

4.10 ACS DOOR MANAGEMENT

4.10.1 The ACS shall support the configuration and management of doors. A user shall be able to add, delete, or modify a door if he or she has the appropriate privileges.

4.10.2 The ACS shall permit multiple access rules to be associated to a door.

4.10.3 The ACS shall support the following forms of authentication: Card Only, Card or Keypad (PIN), or Card and Keypad (PIN). It shall be possible to define a schedule for when Card Only or Card and Keypad authentication modes shall be required.

4.10.4 It shall be possible to set an extended grant time on a per-door basis (in addition to the standard grant time). Cardholder properties shall include the option of using the extended grant time. When flagged cardholders are granted access, the door shall be unlocked for the duration of the extended grant time instead of the standard grant time.

4.10.5 The ACS shall allow the configuration of the relocking mode on doors such as on door open, after a definite time, or on door close.

4.10.6 The ACS shall support the ability to enforce the use of two valid reads from different cardholders to grant access to an area.

4.10.7 The ACS shall support the ability to enable access rules for other cardholders once a supervisor has accessed an area.

4.10.8 The ACS shall support the ability to enable unlocking schedule on a door once an employee has entered the facility.

4.10.9 Unlocking schedules and exceptions to unlocking schedules shall be associated with a door. An unlocking schedule shall determine when a door should be automatically unlocked. The ACS shall also support the use of a specific offline unlocking schedule. Exceptions to unlocking schedules shall be used to define time periods during which unlocking schedules shall not be applied, such as during statutory holidays.

4.10.10 The ACS shall support one or more cameras per door. Video shall then be associated to door access events, such as access grant or access denied.

4.11 ACS CUSTOM FIELDS (USER-DEFINED FIELDS)

4.11.1 The ACS shall permit the creation of custom fields. Up to 1,000 custom fields shall be supported.

4.12 ACS IMPORT TOOL

4.12.1 The ACS shall support an integrated Import Tool to facilitate the import of existing cardholder and credential data. The import of data shall be through the use the CSV file format. The tool shall be available from the Configuration UI.

4.12.2 The Import Tool shall also support the ability to manually import data that has been exported from a third party database if it is in CSV format.

4.12.3 The import tool shall permit the import of the following data:

4.12.3.1 Cardholder name, descriptions, picture, email, and status.

4.12.3.2 Cardholder group information.

4.12.3.3 Credential name, status, format, and card number (including credentials with custom formats).

4.12.3.4 Partition information.

4.12.3.5 Custom fields.

4.12.4 Full flexibility in selecting the fields to be imported during an import session shall be available.

4.12.5 The option to use a custom and unique cardholder key shall be specified during the import process to ensure that cardholders with duplicate names will not have their data overwritten. Cardholder key generation shall be automated. The end user shall have the option to select which fields will be used to create this unique key, e.g. credential number, custom fields, cardholder name.

4.12.6 The ACS shall also support re-importing a CSV file containing new information to update existing information in the ACS database. Re-importing shall enable bulk amendments to existing access control data.

4.13 GENERAL CLIENT SOFTWARE REQUIREMENTS

4.13.1 The Client Software Applications (CSA) shall provide the user interface for USP configuration and monitoring over any network and be accessible locally or from a remote connection.

4.13.2 The CSA shall consist of the Configuration UI for system configuration and the Monitoring UI for monitoring. The CSA shall be Windows-based and provide an easy-to-use graphical user interface (UI).

4.13.3 The CSA for monitoring shall support running in 64-bit mode.

4.13.4 The Server Administrator shall be used to configure the server database(s). It shall be web-based and accessible locally on the SSM or across the network.

4.13.5 The CSA shall seamlessly merge access control and video functionalities within the same user application.

4.13.6 All applications shall provide an authentication mechanism, which verifies the validity of the user. As such, the administrator (who has all rights and privileges) can define specific access rights and privileges for each user in the system.

4.14 CONFIGURATION USER INTERFACE (UI)

4.14.1 The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration. The Configuration UI shall provide decentralized configuration and administration of the USP system from anywhere on the IP network.

4.15 ACS CLIENT USER INTERFACE (UI)

4.15.1 The Monitoring UI shall fulfill the role of a Unified Security Interface that is able to monitor video, ALPR, and access control events and alarms, as well as view live and recorded video.

4.15.2 The Monitoring UI shall provide a graphical user interface to control and monitor the USP over any IP network. It shall allow administrators and operators with appropriate privileges to monitor their unified security platform, run reports, and manage alarms.

4.16 SERVER ADMINISTRATOR USER INTERFACE REQUIREMENTS

4.16.1 The Server Administrator shall be used to configure the SSM and the Directory Role (main configuration) and its database(s), to apply the license, and more.

4.16.2 The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.

4.16.3 Access to the Server Administrator shall be protected via login name, password, and encrypted communications.

4.16.4 The Server Administrator shall allow the administrator (user) to perform the following functions:

4.16.4.1 Manage the system license.

4.16.4.2 Configure the database(s) and database server for the Directory Role,

4.16.4.3 Activate/Deactivate the Directory Role.

4.16.4.4 Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.

4.16.4.5 Define the client-to-server communications security settings. Configure the network communications hardware, including connection addresses and ports.

4.17 UNIFIED WEB CLIENT (UWC) GENERAL REQUIREMENTS

4.17.1 The USP shall support a unified web client (UWC) for access control and video.

4.17.2 The UWC shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.

4.17.3 The UWC shall be platform independent and run within Microsoft Internet Explorer, Firefox, Safari, and Google Chrome.

4.17.4 The UWC shall be designed as an HTML5 application.

4.17.5 The UWC will support native H.264 video in the web client.

4.17.6 Web pages for the web client shall be managed and pushed by the Web Client Server. Microsoft IIS or any other web hosting service shall not be required given that all the web pages shall be hosted by the Mobile Server.

4.17.7 The Web Client Server shall provide the ability to define a unique URL to access the web client, to ensure the security of the application.

4.17.8 The UWC shall provide the ability to configure, save, and reload camera layouts.

4.17.9 The UWC shall provide the ability to control PTZ cameras.

4.17.10 Functionalities:

4.17.10.1 Login using name and password

4.17.10.2 Encrypted communications for all transactions.

4.17.10.3 Print reports and export to CSV file.

4.17.10.4 Customer logo customization shall be available for multi-tenant and hosted services applications.

4.17.10.5 Access Control

4.17.10.5.1Cardholder and group (add/modify/delete).

4.17.10.5.2Credential management (modify/delete).

4.17.10.5.3Visitor management (check-in/modify/check-out).

4.17.10.5.4Unlock door.

4.17.10.5.5Door Activities report.

4.17.10.6 Alarm report

4.18 SMARTPHONE AND TABLET APP GENERAL REQUIREMENTS

4.18.1 The USP shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the USP over any WiFi or mobile network connection.

4.18.2 Mobile apps shall communicate with the USP via a Mobile Server (same as the Unified Web Client or UWC). Communication between the mobile device and the Mobile Server shall support optional encryption.

4.18.3 Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):

4.18.3.1 Apple iPod Touch, iPhone, and iPad.

4.18.3.2 Android-compatible smartphones and tablets.

4.18.3.3 Windows and Windows Phone 8.1.

4.18.4 It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play, Windows Store).

4.18.5 Functionalities

4.18.5.1 Live monitoring and command and control of the USP.

4.18.5.2 Control of camera PTZ.

4.18.5.3 Receive alarm push notifications from the Apple Push Notification Server or from the Google Android push server.

4.18.5.4 Alarm management (view and acknowledge alarms, video tied to alarms).

4.18.5.5 View USP hierarchy and search for entities.

4.18.5.6 Digital zoom on cameras.

4.18.5.7 Support for adaptive resolution scaling.

4.18.5.8 Save camera layouts.

4.18.5.9 Picture-in-picture to view live video when doing playback.

4.18.5.10 View up to 20 cameras simultaneously on iPads.

4.18.6 Access Control

4.18.6.1 View cardholder picture with access-related events.

4.18.6.2 Monitor door status.

4.18.6.3 Unlock door.

4.18.6.4 Override unlocking or locking schedule.

4.18.6.5 Set door in maintenance mode.

4.18.7 Health Monitor

4.18.7.1 The USP shall monitor the health of the system, log health-related events, and calculate statistics.

4.18.8 USP Access Control, Video, and ALPR Unification

4.18.8.1 The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ACS, VMS, and ALPR. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.

4.18.8.2 The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.

4.18.8.3 The user shall be able to associate one or more video cameras to the following entity types: areas, doors, elevators, zones, alarms, intrusion panels, ALPR cameras, and more.

4.18.8.4 It shall be possible to view video associated to access control events when viewing a report.

4.18.8.5 It shall be possible to view video associated to intrusion panel events when viewing a report.

4.18.8.6 It shall be possible to view video associated to ALPR events when viewing a report.

4.18.9 USP Alarm Management

The USP shall support the following Alarm Management functionality:

4.18.9.1 Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.

4.18.9.2 Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.

4.18.9.3 Set the priority level of an alarm and its reactivation threshold.

4.18.9.4 Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.

4.18.9.5 Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.

4.18.9.6 Provide the ability to group alarms by source and by type.

4.18.9.7 Define the time period after which the alarm is automatically acknowledged.

4.18.9.8 Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.

4.18.9.9 Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.

4.18.9.10 Define whether to display the source of the alarm, one or more entities, or an HTML page.

4.18.9.11 Specify whether an incident report is mandatory during acknowledgment.

4.19 USP REPORTING

4.19.1 The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.

4.19.2 Each and every report in the system shall be a USP task, each associated with its own privilege. A user shall have access to a specific report task if he or she has the appropriate privilege.

4.19.3 The USP shall provide the following types of reports:

4.19.3.1 Alarm reports.

4.19.3.2 Video-specific reports (archive, bookmark, motion, and more).

4.19.3.3 Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more).

4.19.3.4 Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more).

4.19.3.5 ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).

4.19.3.6 Health activity and health statistics reports.

4.19.3.7 Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.

4.19.3.8 Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports.

4.19.4 Generic Reports, Custom Reports and Report Templates

4.19.4.1 The user shall the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.

4.19.4.2 The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).

4.19.4.3 All report templates shall be created within the Monitoring UI.

4.19.4.4 These templates can be used to generate reports on a schedule in PDF or Excel formats.

4.19.4.5 An unrestricted number of custom reports and templates shall be supported.

4.19.5 The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.

4.20 USP USER AND USER GROUP SECURITY, PARTITIONS, AND PRIVILEGES MANAGEMENT

4.20.1 The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if he or she has the appropriate privileges.

4.20.2 Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups. User group nesting shall be allowed.

4.20.3 User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR, shall have associated privileges.

4.20.4 Specific entities, such as cardholders, cardholder groups, and credentials shall include a more granular set of privileges, such as the right to access custom fields and change the activation or profile status of an entity.

4.21 USP AUDIT AND USER ACTIVITY TRAILS (LOGS)

4.21.1 The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

4.21.2 Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.

4.21.3 For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.

4.21.4 The USP shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the USP such as login, camera viewed, ALPR event viewed, badge printing, video export, and more.

4.21.5 The ACS shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.

4.22 READERS

4.22.1 Access readers will be semi-flush and/or surface mounted, multi-technology devices incorporating at minimum, 13.56 MHz proximity (smart card) and 125 KHz proximity technology. In high security areas, multi-technology card readers with two-factor authentication including PIN code entry will be required. The access readers will indicate status of badge reads via LED status lights.

4.22.2 The badges will be printable 13.56 MHz proximity PVC cards with vertical slot punched for a badge strap.

4.22.3 Readers and System will support both the existing RICC 125 format and the existing Garrahy Courthouse 13.56 HID iClass SE format.

4.23 CREDENTIALS

4.23.1 Credentials Shall Support the Following:

1. General:
   a. Passive Operation: Credentials must be powered by the reader and not make use of a battery
   b. Use the Client’s Corporate 1000 format
   c. Operating Temperature Range: -40 to 150 degrees F (-40 to 65 degrees C)
   d. Humidity: 0 – 95% non-condensing
   e. Credential coding shall support up to 64 bits
   f. Wiegand Data Configuration
   g. Frequency: 13.56 iClass SE Credential Technology Support

2. PSI-4 Printable Proximity Card:
   a. Dimensions: 3.3 x 2.1 x 0.046 inches (86 x 54 x 0.84 mm)
   b. Slot Punch Indicators: Vertical and Horizontal
   c. Read Range: Up to 7 inches (176 mm)
   d. Finish:
      1) Front: Printable gloss white
      2) Back: Printable gloss white with slot punch indicators
   e. Printing: Front and back surfaces suitable for edge-to-edge dye sublimation printing

5 Cabling and Pathways

5.1 GENERAL

The contractor shall be responsible for completing the following tasks:

5.1.1 Installation, termination, documentation and testing of copper and fiber cabling for device, station and riser cables.

5.1.2 Installation of cable, conduit, faceplates, outlet boxes, and other components.

5.1.3 Core drilling between floors as part of the construction of a routing path for station and riser cables. Installation of riser sleeves and firestopping at all required openings.

5.1.4 Installation of riser and station EMT conduit, sleeves and appropriate firestopping at all wall penetrations.

5.1.5 Installation of equipment racks and cable trays utilized in routing cable.

5.1.6 Provisioning of required electrical power management (PDUs) to the equipment racks.

5.2 LOW VOLTAGE CABLING

5.2.1 All cabling required for proper functioning of the proposed equipment shall be provided and installed by Contractor.

5.2.2 Outlet and camera counts and locations are shown on the attached one-line and coverage drawings.

5.2.3 All data cabling for network devices, IP cameras, and any other IP based communications shall be Category 6A cable.

5.2.4 Other low voltage cables shall be specified by the Contractor. Include cut sheets for each type.

5.2.5 All Cat 6A cable shall be terminated at the serving IDF / BDF on modular color coded Cat6A compliant patch panels, and mounted in wall mount or free standing rack. Include horizontal and vertical cable management.

5.2.6 Equipment racks shall be sized to include all equipment for new system, plus 4U for UPS and switching (provided by others), and minimum 4U spare.

5.2.7 Rack diagrams MUST be submitted by contractor for approval by owner for all equipment racks prior to installation. Propose a logical layout that provides some separation of feeder cables, station cables (voice, data, other/misc), leaving spare slots for growth, and sufficient space for network switches.

5.2.8 Cable and termination components shall carry a manufacturer certification and minimum 15-year system performance guaranty from the manufacturer.

5.2.9 Fiber cabling shall be terminated with LC or SC connectors, and tested and certified with 15 year warranty from manufacturer.

5.2.10 Miscellaneous Cabling:

5.2.10.1 In addition to the camera and access control device cabling, provide and install the miscellaneous telecommunications / data cables as shown on the attached tel/data one-line, including:

Cat 6A station cables (2 per outlet) for the office area
Cat 6A station cables to elevator machine rooms
Fiber and Cat 6A riser feeds between the BDF and IDF, and
Fiber feed to the Courthouse.

5.2.11 Cost Information: Be sure to itemize costs for this work, and show subtotal as “**Low Voltage Cabling**”, in the cost section.

5.3 CONDUITS AND PATHWAYS

5.3.1 All runs shall be enclosed in conduit. No exposed cabling.

5.3.2 All conduits will be sized and constructed so that, after installation of the new cable plant (fiber and copper), the sleeves or conduits fill density will not exceed 40% of capacity.

5.3.3 All cable pulls in conduit shall have pull string left in place for future use. All cables and pull strings will have a permanent label affixed identifying the location of the opposite end of the pull string.

5.3.4 All device cable runs shall be homerun to the serving IDF or BDF. No splices or transition points are allowed unless specifically approved in writing by the Owner.

5.3.5 Station cables may be consolidated in conduits, provided those conduits are properly sized as specified herein to not exceed 40% fill.

5.3.6 Cost Information: Be sure to itemize costs for this work, and show subtotal as “**Conduits and Pathways**”, in the cost section.

5.4 SUBCONTRACTORS

5.4.1 Contractor must identify any portions of the work that will be subcontracted to another entity for completion (i.e. electrical work, conduit installation, fiber or copper terminations, etc.). Subcontractors must be identified by company name, and references provided.

5.5 ELECTRONICS

5.5.1 The Owner will be issuing a separate contract or contracts for some of the network electronics supporting the building. Contractor shall be responsible for coordinating with any electronics installation contractors, to ensure that the infrastructure installed under this contract and the electronics installed by others integrate smoothly, and work proceeds according to the construction schedule.

6 Execution

6.1 PLANNING AND SCHEDULES

6.1.1 Prepare and include an estimated project plan and schedule. Graphically show the sequence and interdependence of each activity. Submit this schedule / work plan as part of Contractor response.

6.1.2 Within fifteen (15) days of receiving Notice to Proceed, the Contractor shall develop and submit a detailed cost loaded project schedule, and schedule of values in a format approved by the Customer's project manager (CPM) for his or her approval.

6.1.3 The schedule will be the key document in determining most financial aspects of the project's execution (payments, liquidated damage, etc.)

6.1.4 The project schedule shall include, but is not limited to, an outline of the tasks that must be completed to satisfy all requirements contained in the RFP and contract documents, as well as, the names and responsibilities of all key participants involved in each task.

6.1.5 The installation must be scheduled to allow for continuous, revenue-collecting operations of the Parking Facilities. Some installation work will need to occur during off-peak hours.

6.1.6 The project schedule shall include completion dates for each task or subtask. The preliminary project schedule and milestones will be attached as part of the contract agreement. Tasks having shared responsibilities that may be outside of the Contractor's direct control or require customer decision making shall be included in the Contractor provided schedule and the CPM will assist the Contractor in procuring the necessary information.

6.1.7 The project schedule shall be organized by phase or sub phase (corresponding to a parking facility) and shall include milestones (action and date) for each facility and a level of detail down to the individual lane in each facility. If the Contractor requests to run phases or sub-phases concurrently the Contractor shall provide for separate tracking (to the lane level) for the multiple tasks in process.

6.1.8 The Contractor shall provide overall operational completion dates for each phase or sub-phase. The Contractor's failure e to meet the milestone dates for the individual phase or sub-phase completion dates shall invoke liquidated damages.

6.1.9 The Contractor's project manager shall be responsible for maintaining the schedule for the duration of the project (with regular updates as required by the CPM) and will inform the CPM of significant foreseeable changes to the schedule at least two weeks before the expected event is to take place. Unforeseen changes shall be reported immediately upon discovery.

6.1.10 In the event of such a delay the Contractor's project manager shall be responsible for identifying and proposing methods to get the project back on schedule (or to expedite the schedule) and for making appropriate changes to the schedule, as approved by the CPM.

6.1.11 The Contractor's project manager shall also be responsible for communicating any schedule changes (through channels or methods approved by the CPM) to all parties that may be impacted by the change.

6.2 EXAMINATION

6.2.1 Examine cable pathways including conduit, raceways, cable trays, and other pathway elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

6.2.2 Examine rough-in for control cable and conduit systems to controllers, card readers, and other system components to verify conduit and back-box locations prior to installation of system devices

6.2.3 Examine install location for compliance with space allocations, installation tolerance, hazards to safe system operation, and other conditions affecting installation

6.2.4 Examine roughing-in for LAN, WAN, and IP network before device installation

6.2.5 Examine available network capacity and support infrastructure. Consult with network administrator for compliance with network standards and capacity

6.3 PREPARATION

6.3.1 Prior to beginning video system programming, prepare detailed project planning forms for programming and configuration of the system. Fill in all data available from project plans and specifications and publish as project planning documents for review and approval. These may include (but are not limited to):

6.3.1.1 Define user (operator) types

6.3.1.2 Define camera naming schema

6.3.1.3 Determine storage requirements

6.3.1.4 Determine FPS requirements

6.3.1.5 Determine motion recording

6.3.1.6 Define event programming

6.3.1.7 Develop matrix layouts

6.3.1.8 Prepare a project specific plan for system testing, startup, and demonstration

6.3.1.9 Develop cable and asset-management system labeling plan

6.3.2 Prior to beginning access control system programming, prepare detailed project planning forms for programming and configuration of the system

6.3.3 Comply with SIA CP-01 Control Panel Standard.

6.3.4 Comply with ANSI/TIA-606-B Labelling Standard.

6.3.5 Prepare detailed project planning forms for programming and configuration of the SMS. Fill in all data available from project plans and specifications and publish as project planning documents for review and approval. These may include (but are not limited to):

6.3.5.1 Define SMS Partitions.

6.3.5.2 For each Location, record setup of controller features and access requirements.

6.3.5.3 Propose start and stop times for time zones and holidays, and match up access levels for doors.

6.3.5.4 Set up groups, facility codes, software triggers, and list inputs and outputs for each SMS Controller.

6.3.5.5 Assign action message names and compose messages.

6.3.5.6 Set up alarms. Establish trigger actions between events and video surveillance features.

6.3.5.7 Prepare and install alarm graphic maps.

6.3.5.8 Develop user-defined fields.

6.3.5.9 Develop screen layout formats.

6.3.5.10 Discuss badge layout options; design badges.

6.3.5.11 Complete system diagnostics and operation verification.

6.3.5.12 Prepare a specific plan for system testing, startup, and demonstration.

6.3.5.13 Develop acceptance test concept and, on approval, develop specifics of the test.

6.3.5.14 Develop cable and asset-management system details; input data from construction documents. Include system schematics and technical drawings in electronic format.

6.3.6 In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final programming and configuration documents. Use final documents to program and configure software.

6.4 PRE-CUT TESTING

6.4.1 Contractor shall draft and provide a customized and detailed test plan to verify the proper operation of the system and its various functions.

6.4.2 Prior to receiving final authorization to go live, the vendor will complete the entire battery of tests on all systems in the presence of the owner and / or his CPM. These tests must pass flawlessly.

6.5 CUTOVER ACTIVITIES

6.5.1 The Customer reserves final approval on any cutover scheduling.

6.5.2 Contractor will then be responsible for transitioning equipment, software and systems into production service.

6.5.3 Upon completion of cutover activities, any equipment that has been replaced and is no longer in use will be collected and disposed of by the contractor.

6.5.4 Cabling that is no longer in use shall be removed. Cable that is in good condition and that could be re-tasked for other functions may, with written approval from Customer, remain in place, coiled and properly labeled for future use.

7 Warranty, Training and Support:

7.1 POST-CUTOVER SUPPORT:

7.1.1 Provide for help desk function and coverage to assist customer staff with feature changes and trouble clearing for up to three weeks after cutover.

7.2 TRAINING

7.2.1 User Guides

7.2.1.1 The vendor will take responsibility for delivering user training and system use guideline documents in a timely fashion for distribution prior to training and cutover. Electronic versions are acceptable. Materials should be customized to include any Customer specific features and procedures, and Customer logo or other info.

7.2.2 Operator training

7.2.2.1 Live staff training classes for the users will be conducted. Customer must approve the training format, materials and training staff. Training staff is to be supplied by the vendor as part of the contract.

7.2.2.2 Training shall cover the basics of system operations in detail, and also go through some of the new features (as compared to previous system).

7.2.2.3 Divide training classes and customize by job functions. (E.g., security staff may need different training than supervisory personnel, or back office financial staff.

7.2.2.4 Proposer shall provide thirty hours (30) minimum of training time during a one-month period, followed by another fifteen hours (15) of refresher training to be scheduled within 30 days of acceptance. Per day pricing for additional training shall also be included.

7.2.2.5 Proposer shall maintain records of the training periods given. Any part of the initial period of 45 hours training not utilized prior to the end of system commissioning shall be available for future training of the Customer's representatives during the first twelve months of operation.

7.2.2.6 Proposer shall offer the option of additional periods of training, each period being of a maximum of 20 hours, at any time during the first five (5) year period of equipment maintenance.

7.3 ONGOING SUPPORT AND SERVICE REQUIREMENTS

7.3.1 Service Calls

7.3.1.1 In the case of any malfunction, the time to repair shall be limited to four (4) hours, 2 hour response time and 2 hour repair time, for faults reported during normal contract hours. For calls outside contract hours, maximum time to repair shall not exceed 24 hours. However, if an after-hours trouble report is reported as an emergency, then the standard 2-hour response / 4-hour to repair shall apply, but vendor may include charges for overtime rates for the work.

7.3.1.2 No equipment, system, or component shall be left non-operable after a 24-hour period following notification by the Customer.

7.3.1.3 Saturdays, Sundays and holidays are normal business days for Customer and should be included in the expected repair warranty coverage.

7.3.2 Warranty

7.3.2.1 All equipment shall be covered by a manufacturer's warranty via the Proposer, covering all parts and labor for a two (2) year period, excluding misuse or vandalism.

7.3.2.2 The warranty period will start once the equipment is installed, operational, and is accepted in writing by Customer. This customer acceptance will be triggered after customer and vendor have completed the full battery of pre-service tests, the system is fully in service and operational, and has operated without any malfunctions or trouble reports for a period of three continuous weeks. Any malfunctions during the acceptance period will reset the clock and start a new 21 day acceptance period.

7.3.2.3 During the warranty period, software modifications (upgrades) that improve the functionality of the system shall be provided to the owner at no additional cost.

7.3.2.4 All warranties are to be delivered to the Customer prior to commencement of the warranty period.

7.3.2.5 Preventative maintenance to be carried out on a cyclic basis, with appropriate equipment functions being checked monthly or more frequently if necessary. Documentation shall be made available for customer inspection on site.

7.3.2.6 Software update and error correction shall be provided as part of the service support function, so that the system is not outmoded or disadvantaged in terms of reliability, spares availability, and repair diagnosis.

7.3.3 Maintenance Contract

7.3.3.1 The Customer wishes to secure a long term maintenance and support agreement with the successful vendor. Please provide itemized pricing to extend the coverage period beyond the two-year warranty period by:

7.3.3.1.1 Three years, for a **total of five years** from acceptance

7.3.3.1.2 Annual renewal, year by year, starting after year 2, for up to five (5) 1-year renewals.

7.3.3.2 Be sure to note clearly if there are any additional required or optional manufacturer support or maintenance components (such as Software Support, etc.) that should be included. All maintenance options or components should be clearly identified and itemized.

7.3.3.3 Equipment or parts to be excluded from the maintenance contract are to be defined, together with estimates of operational life and replacement costs.

7.3.4 Transition of maintenance contract to new vendor

7.3.4.1 It is expected that at some date beyond the warranty period initial term, or subsequent renewals, Customer will seek to forge a new maintenance agreement.

7.3.4.2 To facilitate this process, which may include a transition to a new contractor, Customer may wish to move to a month-to-month contract for some period not to exceed 1 year. This month-to-month option shall be offered by the Contractor under the same terms and conditions and costs without penalty.

Appendix A: Camera Specifics

4MP High Resolution PTZ IP Cameras - AXIS Q1786-LE

a. Outdoor-ready 4-megapixel resolution and 32x optical zoom. These cameras shall be equipped with:
   1. Wide dynamic range feature maximal forensic usability to handle scenes with strong variations in light, capture full-color images in extremely low light.
   2. Built-in IR illumination with automatic adaptive feature, providing exceptional video quality in any light conditions.
   3. Supports technology that significantly reduces bandwidth and storage requirements.
   4. Vandal-resistant housing with IK10 rating.
   5. Remote zoom and focus

b. Camera general parameters:
   1. Image Sensor: 1/1.8" progressive scan RGB CMOS
   2. Lens:
      a. 4.3–137 mm, F1.4–4.0
      b. Horizontal field of view: 60°- 2.3°
      c. Vertical field of view: 39°–1.3°
      d. Autofocus, automatic day/night
      e. Thread for 62 mm filters, max filter thickness: 5 mm
   3. Day and night: Automatically removable infrared-cut filter in day mode and infrared-pass filter 720 nm in night mode
   4. Minimum illumination:
      a. Color: 0.18 lux at 50 IRE, F1.4
      b. B/W: 0.04 lux at 50 IRE, F1.4, 0 lux with IR illumination
   5. Shutter time: 1/100000 s to 2 s

c. Video parameters:
   1. Video compression:
      a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
      b. Motion JPEG
   2. Resolution: 2560x1440 to 160x120,
      a. Maximum pixel density with 32x optical zoom:
         i. 25 m (82 ft): 2551 px/m
         ii. 50 m (164 ft): 1275 px/m
         iii. 250 m (820 ft): 255 px/m
   3. Frame rate:
      a. With WDR: Up to 25/30 fps (50/60 Hz) in all resolutions
      b. Without WDR: Up to 50/60 fps (50/60 Hz) in all resolutions
   4. Video streaming:
      a. Multiple, individually configurable streams in H.264
      b. Motion JPEG
      c. Bandwidth reduction technology in H.264
      d. Controllable frame rate and bandwidth
      e. VBR/MBR H.264
   5. Multi-view streaming:
   6. Pan/Tilt/Zoom: 32x optical zoom, preset positions
   7. Image settings:
      a. Compression, Color, Brightness, Sharpness, Contrast, Local contrast, White balance.
      b. Exposure control (including automatic gain control), Exposure zones.
      c. Fine tuning of behavior at low light.
      d. Wide Dynamic Range: up to 120 dB depending on scene.

e. Text and image overlay, Mirroring of images, Privacy masks.
f. Rotation: 0°, 90°, 180°, 270°, including Corridor Format

d. Network Parameters
1. Security:
a. Password protection.
b. IP address filtering.
c. HTTPSa encryption.
d. IEEE 802.1Xa network access control.
e. Digest authentication.
f. User access log.
g. Centralized certificate management.
h. Brute force delay protection.
i. Signed firmware
2. Supported network protocols: IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, LLDP

e. System integration
1. Application Programming Interface:
a. Open API for software integration.
b. ONVIF® Profile G.
c. ONVIF® Profile S.
d. ONVIF® Profile T specification at onvif.org

f. Analytics support including: Video motion detection, fence guard, loitering guard, motion guard, active tampering alarm, gatekeeper

g. General camera parameters
1. Casing:
a. IP66- and NEMA 4X-rated
b. IK10 impact-resistant casing with hard-coated dome and dehumidifying membrane
c. Encapsulated electronics and captive screws
d. Color: white NCS S 1002-B
e. Availability of repainting option
2. Sustainability: PVC free 2% Recycled Plastic
3. Memory: 1 GB RAM, 512 MB Flash
4. Power:
a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3,max 11.5 W, typical 8.6 W
5. Connectors:
a. RJ45 10BASE-T/100BASE-TX PoE
6. IR illumination:
a. Power-efficient, long-life 850 nm IR LED's with adjustable angle of illumination and intensity. Range of reach 30 m (98 ft) in wide field of view and 80 m (262 ft) in full tele view, or more depending on the scene
7. Storage:
a. Support for microSD/microSDHC/microSDXC card
b. SD card encryption
c. Support for recording to network-attached storage (NAS)
8. Operating conditions:
a. Operation: -40 °C to 60 °C (-40 °F to 140 °F)
b. Humidity 10 to 100% RH (condensing)
9. Storage conditions:
a. -40 °C to 65 °C (-40 °F to 149 °F)

b. Humidity 5-95% RH (non-condensing)

10. Approvals:
    a. EMC
        i. EN 55032 Class B, EN 50121-4, IEC 62236-4
        ii. EN 55024, EN 61000-6-1, EN 61000-6-2
        iii. FCC Part 15 Subpart B Class A and B, ICES-003 Class B
        iv. VCCI Class B, RCM AS/NZS CISPR 22 Class B, KCC KN32 Class B
        v. KN35
    b. Safety
        i. IEC/EN/UL 60950-1, IEC/EN/UL 60950-22, IEC/EN 62471
        ii. IS 13252
    c. Environment
        i. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14
        ii. IEC 60068-2-6 (vibration), IEC 60068-2-27 (shock)
        iii. IEC 60068-2-30, IEC 60068-2-78, IEC/EN 60529 IP66
        iv. NEMA 250 Type 4X, IEC/EN 62262 IK10
    d. Network
        i. NIST SP500-267
11. Weight: 2.4 Kg (5.3 lb)

2.1.25 HDTV 1080p High Resolution IP Cameras - AXIS P3245-LVE

a. Outdoor-ready in HDTV 1080p. These cameras shall be equipped with:
    1. HDTV 1080p video quality
    2. Low-light technology, forensic WDR and power efficient built-in IR
    3. Reduced bandwidth and storage needs supporting H.264 and H.265
    4. Signed firmware and secure boot

b. Camera general parameters:
    1. Image Sensor: Progressive scan RGB CMOS 1/2.8"
    2. Lens:
        a. Varifocal, 3.4–8.9 mm, F1.8
        b. Horizontal field of view: 100°-36°
        c. Vertical field of view: 53°–20°
        d. Remote zoom and focus, P-Iris control, IR corrected
    3. Day and night: Automatically removable infrared-cut filter
    4. Minimum illumination:
        a. Color: 0.1 lux at 50 IRE, F1.8
        b. 0.02 lux at 50 IRE, F1.8; 0 lux with IR illumination on
    5. Shutter time: 1/66500 s to 2 s
    6. Camera angle adjustment: Pan ±180°, tilt ±75°, rotation ±175°

c. Video parameters:
    1. Video compression:
        a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
        b. H.265 (MPEG-H Part 2/HEVC) Main Profile
        c. Motion JPEG
    2. Resolution: 1920x1080 to 160x90
    3. Frame rate:
        a. With WDR: 25/30 fps with power line frequency 50/60 Hz
        b. Without WDR: 50/60 fps with power line frequency 50/60 Hz
    4. Video streaming:
        a. Multiple, individually configurable streams in H.264, H.265, and Motion JPEG
        b. Bandwidth reduction technology in H.264 and H.265

c. Controllable frame rate and bandwidth
d. VBR/MBR H.264/H.265

5. Multi-view streaming: 2 individually cropped out view areas in full frame
6. Pan/Tilt/Zoom: Digital PTZ, Preset positions
7. Image settings:

a. Compression, color saturation, brightness, sharpness, contrast, local contrast, white balance, day/night threshold, tone mapping, exposure control (including automatic gain control), exposure zones, defogging, forensic WDR: up to 120 dB depending on scene, barrel distortion correction, fine tuning of low-light behavior, dynamic text and image overlay, privacy masks, mirroring, rotation: 0°, 90°, 180°, 270°, including corridor format.

d. Network Parameters

1. Security: Password protection, IP address filtering, HTTPS encryption, IEEE 802.1x (EAP-TLS) network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot
2. Supported protocols: IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, SIP, LLDP

e. System integration

1. Application Programming Interface:
   a. Open API for software integration.
   b. ONVIF® Profile G.
   c. ONVIF® Profile S.
2. Analytics support including:
   a. Video Motion Detection, active tampering alarm
   b. Support for Camera Application Platform enabling installation of third-party applications.
3. Event triggers: Analytics, edge storage events, virtual inputs through API
4. Event actions:
   a. Overlay text, video recording to edge storage, pre- and post-alarm video buffering
   b. Video clip file upload via: FTP, SFTP, HTTP, HTTPS, network share and email
   c. Pre- and post-alarm video or image buffering for recording or upload
   d. Notification: email, HTTP, HTTPS, TCP and SNMP trap
   e. Overlay text
5. Data streaming: Event data
6. Built-in installation aids: Remote zoom, remote focus, pixel counter

f. General camera parameters

1. Casing:
   a. IP66- and NEMA 4X-rated
   b. IK10 impact-resistant casing with hard-coated dome and dehumidifying membrane
   c. Encapsulated electronics and captive screws
   d. Color: white NCS S 1002-B
   e. Availability of repainting option
2. Sustainability: PVC free
3. Memory: 1 GB RAM, 512 MB Flash
4. Power:
   a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3,max 11.5 W, typical 8.4 W
5. Connectors:
   a. RJ45 10BASE-T/100BASE-TX PoE
6. IR illumination:

a. Optimization of IR Beam with power-efficient, long-life 850 nm IR LEDs. Range of reach 40 m (130ft) or more depending on the scene

7. Storage :
   a. Support for microSD/microSDHC/microSDXC card
   b. SD card encryption
   c. Support for recording to network-attached storage (NAS)
8. Operating conditions:
   a. Operation: -40 °C to 50 °C (-40 °F to 122 °F)
   b. Start-up: –30 °C to 50 °C (-22 °F to 122 °F)
   c. Maximum temperature (intermittent): 55 °C (131 °F)
   d. Humidity 10 to 100% RH (condensing)
9. Approvals:
   a. EMC
      i. EN 55032 Class A, EN 50121-4, IEC 62236-4, EN 55024, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-3(A)/NMMB-3(A), VCCI Class A, RCM AS/NZS CISPR 32 Class A, KC KN32 Class A, KC KN35
   b. Safety
      i. IEC/EN/UL 60950-1, IEC/EN/UL 60950-22, IEC/EN 62471
   c. Environment
      i. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-30, IEC 60068-2-78
10. Weight: 800 g (1.8 lb) including weather-shield

2.1.26 8.3 MP High Resolution IP Cameras - AXIS P3807-PVE

a. Multi-sensor 8.3 MP High Resolution IP Cameras. These cameras shall be equipped with:
   1. 180° horizontal and 90° vertical coverage
   2. 8.3 MP resolution at full frame rate
   3. Reduced bandwidth and storage needs supporting H.264

b. Camera general parameters:
   1. Image Sensor: 4 x 1/2.9” progressive scan RGB CMOS
   2. Lens:
      a. Varifocal, 3.2 mm, F2.0
      b. Horizontal field of view: 180°
      c. Vertical field of view: 90°
   3. Day and night: Automatically removable infrared-cut filter
   4. Minimum illumination:
      a. Color: 0.17 lux
      b. 0.05 lux
   5. Shutter time: 1/33500 s to 1/10 s
   6. Camera angle adjustment: Pan ±180°, tilt ±0°,35°, 45°, 55°, rotation ±10°

c. Video parameters:
   1. Video compression:
      a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
      b. Motion JPEG
   2. Resolution: 4320x1920 to 480x270
   3. Frame rate:
      a. With WDR: 12.5/15 fps with power line frequency 50/60 Hz
      b. Without WDR: 25/30 fps with power line frequency 50/60 Hz
   4. Video streaming:
      a. 8.3 MP (client dewarp): 1 individually configurable stream in H.264 and Motion JPEG

b. 7.5 MP (dewarped): 2 individually configurable streams in H.264 and Motion JPEG
c. Bandwidth reduction technology in H.264 and H.265
d. Controllable frame rate and bandwidth
e. VBR/MBR H.264

5. Multi-view streaming: 2 individually cropped out view areas in full frame
6. Pan/Tilt/Zoom: Digital PTZ, Preset positions
7. Image settings:

a. Saturation, contrast, brightness, sharpness, Forensic WDR: up to 120 dB depending on scene, white balance, day/night threshold, exposure mode, compression, dynamic text and image overlay, exposure control, noise reduction, fine tuning of behavior at low light, polygon privacy masks

d. Network Parameters

1. Security: Password protection, IP address filtering, HTTPS encryption, IEEE 802.1x (EAP-TLS) network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot
2. Supported protocols: IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, SIP, LLDP

e. System integration

1. Application Programming Interface:
   a. Open API for software integration.
   b. ONVIF® Profile G.
   c. ONVIF® Profile S.
2. Analytics support including:
   a. Video Motion Detection, active tampering alarm
   b. Support for Camera Application Platform enabling installation of third-party applications.
3. Event triggers: Analytics, edge storage events, shock detection
4. Event actions:
   a. Overlay text, video recording to edge storage, pre- and post-alarm video buffering
   b. Video clip file upload via: FTP, SFTP, HTTP, HTTPS, network share and email
   c. Pre- and post-alarm video or image buffering for recording or upload
   d. Notification: email, HTTP, HTTPS, TCP and SNMP trap
   e. Overlay text
5. Data streaming: Event data
6. Built-in installation aids: pixel counter, leveling guide

f. General camera parameters

1. Casing:
   a. IP66-/IP67- and NEMA 4X-rated, IK10-rated impact-resistant casing with polycarbonate hard coated clear dome, aluminum base and dehumidifying membrane
   b. Color: white NCS S 1002-B
   c. Availability of repainting option
2. Sustainability: PVC free
3. Memory: 1 GB RAM, 512 MB Flash
4. Power:
   a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3, Typical 7 W, max 12.9 W
5. Connectors:
   a. RJ45 10BASE-T/100BASE-TX PoE
6. Storage:

a. Support for microSD/microSDHC/microSDXC card
b. SD card encryption
c. Support for recording to network-attached storage (NAS)

7. Operating conditions:
    a. Operation: -30 °C to 50 °C (-22 °F to 122 °F)
    b. Humidity 10 to 100% RH (condensing)
8. Approvals:
    a. EMC
        i. EN 55032 Class A, EN 50121-4, IEC 62236-4, EN 55024, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A, KC KN32 Class A, KC KN35
    b. Safety
        i. IEC/EN/UL 60950-22, IEC/EN/UL 62368-1, IS 13252
    c. Environment
        i. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66/IP67, IEC/EN 62262 IK10, NEMA 250 Type 4X
9. Weight: 2.0 Kg (4.5 lb)

26 5.0MP High Resolution IP Cameras - AXIS Q3517-LVE Network Camera

a. Multi-sensor 8.3 MP High Resolution IP Cameras. These cameras shall be equipped with:
    1. Forensic WDR, built-in IR LEDs with automatic and seamless adapting angle of illumination and intensity
    2. Reduced bandwidth and storage needs supporting H.264

b. Camera general parameters:
    1. Image Sensor: Progressive scan RGB CMOS 1/1.8”
    2. Lens:
        a. Varifocal, 4.3-8.6 mm, F1.5
        b. Horizontal field of view: 96° – 50°
        c. Vertical field of view: 53° – 29°
        d. Remote focus and zoom, P-Iris control, IR-corrected
    3. Day and night: Automatically removable infrared-cut filter
    4. Minimum illumination:
        a. 5MP 25/30 fps with WDR: Color: 0.12 lux at 50 IRE, F1.5; B/W: 0.02 lux at 50 IRE, F1.5, 0 lux with IR illumination on
        b. 4MP 50/60 fps: Color: 0.24 lux at 50 IRE, F1.5, B/W; 0.04 lux at 50 IRE, F1.5, 0 lux with IR illumination on
    5. Shutter time: 1/71500 s to 2s
    6. Camera angle adjustment: Pan ±360°, tilt ±80°, rotation ±175°

c. Video parameters:
    1. Video compression:
        a. H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
        b. Motion JPEG
    2. Resolution: 3072x1728 to 160x120
    3. Frame rate:
        a. 5MP with WDR: 25/30 fps with power line frequency 50/60 Hz
        b. 4MP without WDR: 50/60 fps with power line frequency 50/60 Hz
    4. Video streaming:
        a. Multiple, individually configurable streams in H.264 and Motion JPEG
        b. Controllable frame rate and bandwidth
        c. VBR/MBR H.264
    5. Multi-view streaming: 8 individually cropped out view areas in full frame

6. Pan/Tilt/Zoom: Digital PTZ, Preset positions
7. Image settings:
    a. Scene profiles, compression, color, brightness, sharpness, contrast, local contrast, white balance, day/night threshold, exposure control (including automatic gain control), defogging, exposure zones, fine tuning of behavior at different light levels, Forensic WDR: Up to 120 dB depending on scene, electronic image stabilization, barrel distortion correction, dynamic text and image overlay, privacy masks, mirroring of images, straighten image, rotation: 0°, 90°, 180°, 270°, auto, including corridor format

d. Network Parameters
1. Security: Password protection, IP address filtering, IEEE 802.1X network access control, HTTPS encryption, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware
2. Supported protocols: IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, LLDP

e. System integration
1. Application Programming Interface:
    a. Open API for software integration.
    b. ONVIF® Profile G.
    c. ONVIF® Profile S.
2. Analytics support including:
    a. Video motion detection, motion guard, fence guard, loitering guard, active tampering alarm, audio detection
3. Event triggers: Analytics, supervised external inputs, virtual inputs through API, edge storage events, shock detection
4. Event actions:
    a. Record video: SD card and network share
    b. Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share and email
    c. Pre- and post-alarm video or image buffering for recording or upload
    d. Notification: email, HTTP, HTTPS, TCP and SNMP trap
    e. Overlay text, external output activation, play audio clip, zoom preset
5. Data streaming: Event data
6. Built-in installation aids: Remote zoom, remote focus, pixel counter, leveling assistant, autorotation, straighten image, traffic wizard

f. General camera parameters
1. Casing:
    a. IP66-, IP67-, IP6K9K- and NEMA 4X-rated, IK10+ (50 joules) impact-resistant casing with polycarbonate hard-coated dome, aluminum base and dehumidifying membrane
    b. Encapsulated electronics, captive screws
    c. Color: White NCS S 1002-B
2. Sustainability: PVC free
3. Memory: 1 GB RAM, 512 MB Flash
4. Power:
    a. Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1
    b. Class 3, typical 6.5 W, max 12.9 W
    c. 8–28 V DC, typical 6.9 W, max 14.5 W
    d. Power redundancy
5. Connectors:

a. RJ45 10BASE-T/100BASE-TX PoE, terminal block for two configurable supervised inputs / digital outputs (12 V DC output, max load 50 mA), 3.5 mm mic/line in, 3.5 mm line out, terminal block for DC input

6. Storage:
   a. Support for microSD/microSDHC/microSDXC card
   b. SD card encryption
   c. Support for recording to network-attached storage (NAS)
7. Operating conditions:
   a. Operation: -50 °C to 60 °C (-58 °F to 140 °F)
   b. Humidity 10 to 100% RH (condensing)
8. Approvals:
   a. EMC
      i. EN 55032 Class A, EN 50121-4, IEC 62236-4, EN 55024, IEC/EN 61000-6-1, IEC/EN 61000-6-2, FCC Part 15, Subpart B, Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 22 Class A, KCC KN32 Class A, KN35
   b. Safety
      i. IEC/EN/UL 60950-22, IEC/EN/UL 62368-1, IS 13252
   c. Environment
      i. IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, NEMA 250 Type 4X, IEC/EN 62262 IK10+ (50J), ISO 20653 IP6K9K, IEC/EN 60529 IP66/67
9. Weight: 2.0 Kg (4.4 lb)

Appendix B: Bidder Qualification Form

Rhode Island Convention Center

1 Sabin St, Providence, RI 02903

Electronic Security Systems RFP

Bidder Qualification Form

December 2019

Part 1

Contractor Information

Legal Business Name: ____

Address: ____

Telephone: ____

Owner(s):
____

Primary Bidding Contact: ____

Contact Number: __________________________ Contact Email: __________________________

Part 2

Relevant Work Experience

(Please provide relevant information from projects within the last three years)

PROJECT ONE

Client/Project:
____

Address: ____

Scope: ____

____

____

____

Contact Name: ____

Contact Number: _______________________ Contact Email: ____________________________

Project Start Date: ______________________Completion Date: __________________________

PROJECT TWO

Client/Project:
____

Address: ____

Scope: ____

____

____

____

Contact Name: ____

Contact Number: _______________________ Contact Email: ____________________________

Project Start Date: ______________________Completion Date: __________________________

PROJECT THREE

Client/Project:
____

Address: ____

Scope: ____

____

____

____

Contact Name: ____

Contact Number: ____________________ Contact Email: ________________________

Project Start Date: ___________________Completion Date: ______________________

PROJECT FOUR

Client/Project:
____

Address: ____

Scope: ____

____

____

____

Contact Name: ____

Contact Number: _____________________ Contact Email: ___________________________

Project Start Date: ____________________Completion Date: _______________________

PROJECT FIVE

Client/Project:
____

Address: ____

Scope: ____

____

____

____

Contact Name: ____

Contact Number: _____________________ Contact Email: ___________________________

Project Start Date: ____________________Completion Date: _______________________

Manpower

Number of project dedicated Technicians: ____

Number of project dedicated Project Managers: ____

Able to provide 24/7/365 Emergency Service: (Y / N) ____________________________________

Response Time (Normal Business) Hours:

Returned Phone Call: ____

Certified Technician Onsite: ____

Response Time (Off-Normal Business) Hours:

Returned Phone Call: ____

Certified Technician Onsite: ____

Distance of closest certified staffed service facility from project side in miles: _________________

Will your company outsource / subcontract labor forces for this project? Please Circle (Y / N) ___

(If yes, explain): ____

____

____

____

____

____

____

Part 4

Manufacturer Certifications

(Provide copies of company certification, and technician / installer certifications)

Manufacturer Certification(s):

- Technical Resource Name: ____
  - Certification Type: ____
  - Original Certification date: ____
  - Current Certificate Expiration date: __________________________________

- Technical Resource Name: ____
  - Certification Type: ____
  - Original Certification date: ____
  - Current Certificate Expiration date: __________________________________

- Technical Resource Name: ____
  - Certification Type: ____
  - Original Certification date: ____
  - Current Certificate Expiration date: __________________________________

<Attach additional Sheets as necessary>

Part 5

Insurance

Company Name: ____

Policy Number: ____

Policy Amount: ____

Single Project Bonding Limit: ____

Aggregate Bonding Limit: ____

I attest that the information contained herein is true and accurate at this time, and that I will provide additional verification if requested. Omissions, inaccuracies, OR MISREPRESENTATIONS will render my bid null and void, and may result in the loss of bidding any future BASF work / or considerations.

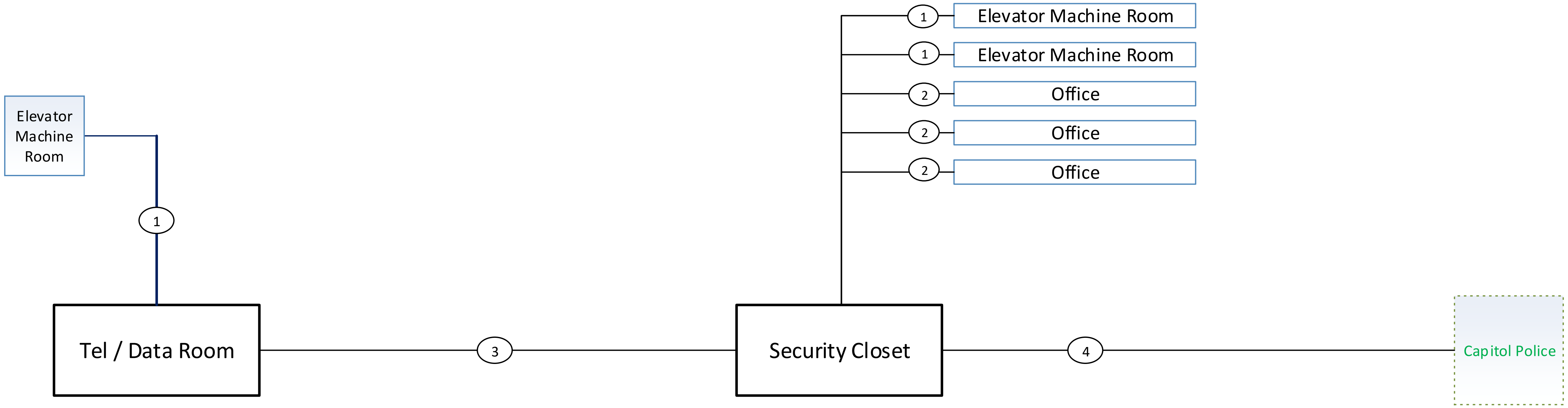
Signature: ____

Name: ____

Title: ____

Date: ____

Appendix C: Drawings



One-Line Symbol Key

1	(1) Cat 6A
2	(2) Cat 6A
3	(6 strand 8.3/125um) SM, (6 strand OM3 50/125um) MM, (6) Cat5e
4	(6 strand OM3 50/125um) MM, (2) Cat6A

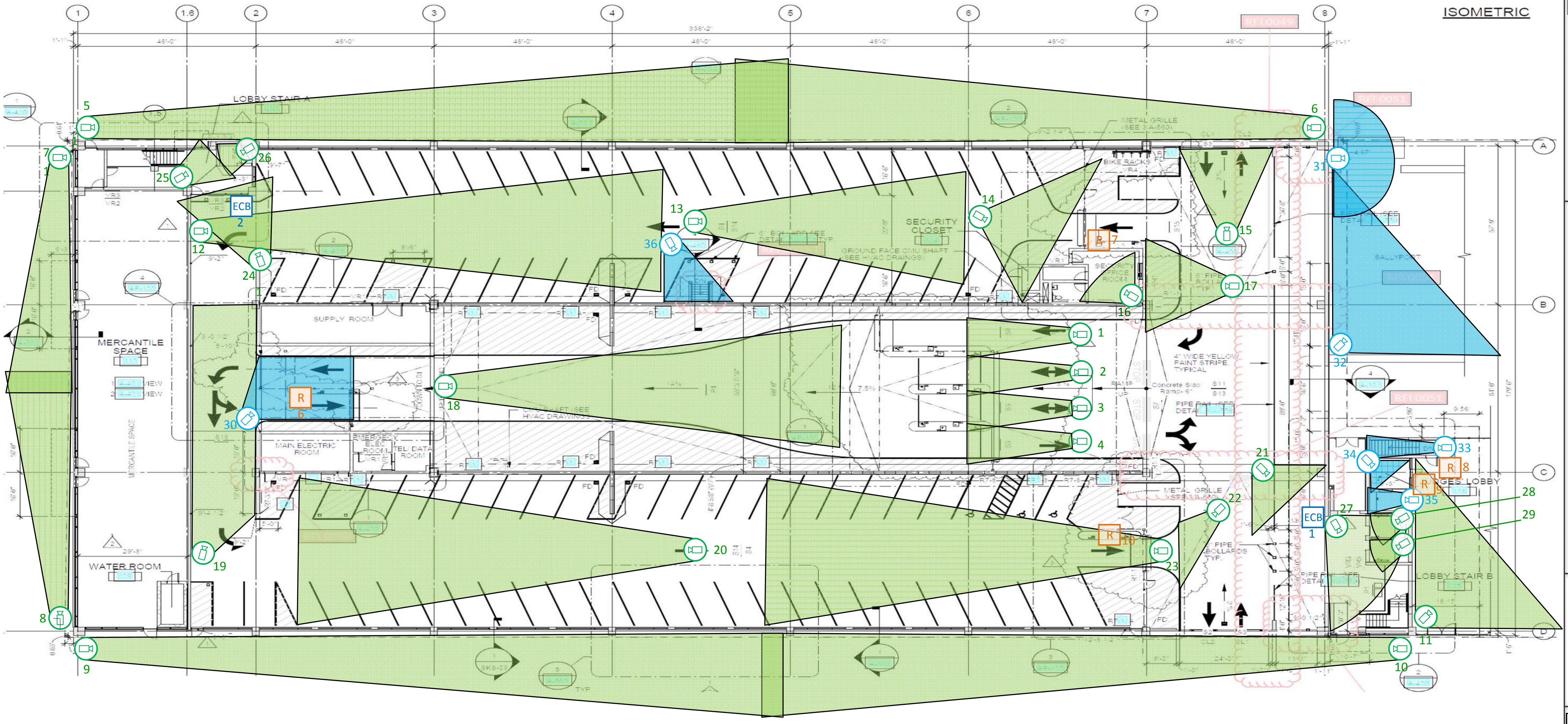
GROUND FLOOR

Garahy Parking Garage

GARRAHY COURTHOUSE
PARKING GARAGE
PROVIDENCE, RI

Engineered by:
Drawn by:
Scale: Not Applicable
Job Number:
Date:
File Name:

Tel/Data Layout



1 GROUND TIER PLAN

Garahy Parking Garage

No#	Revision Description
1	Initial drafts completed

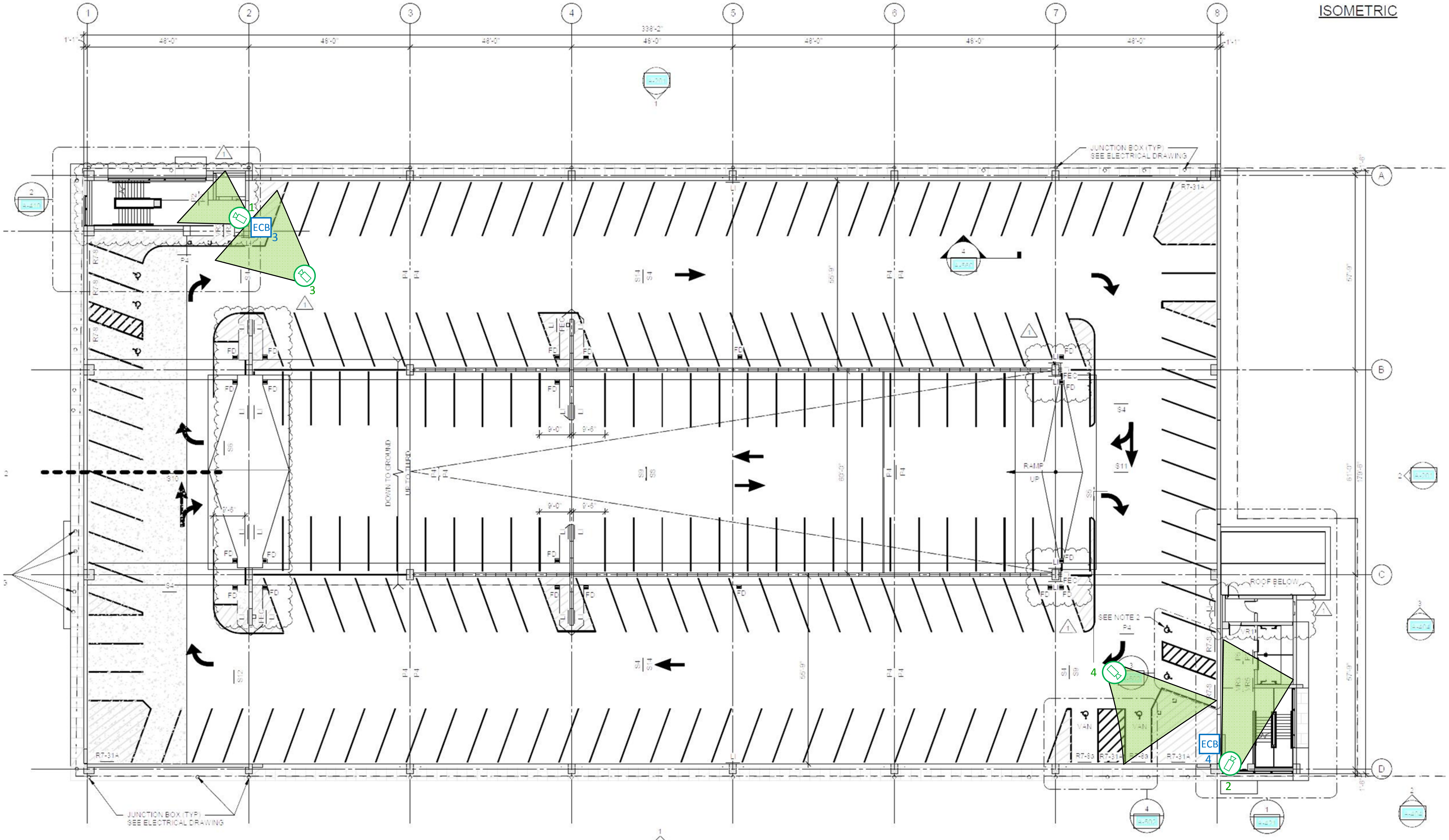
SYM	DESCRIPTION
ECB	EMERGENCY CALL BOX
n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

Engineered by:
Drawn by:
Scale: Not Applicable
Job Number:
Date:
File Name:

Security System Layout



NOTE:
1. FOR TIPICAL WALL SECTION , CALLOUT A-... AND SECTION VIEW SEE SHEET A-104

1 SECOND TO SIX TIER PLAN

Garahy Parking Garage

No#	Revision Description
1	Initial drafts completed

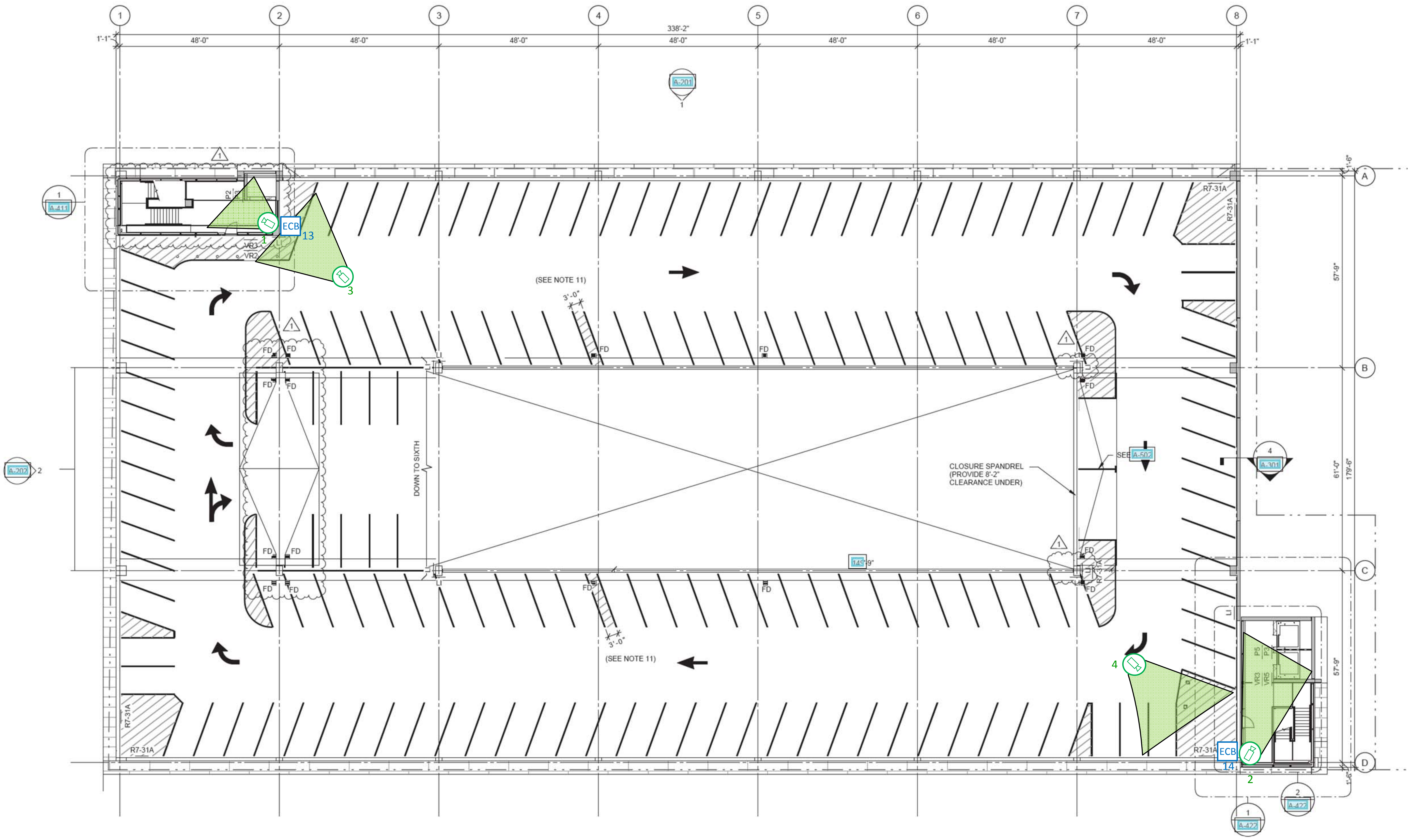
SYM	DESCRIPTION
ECB	EMERGENCY CALL BOX
n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE
PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

Engineered by:	
Drawn by:	
Scale: Not Applicable	
Job Number:	
Date:	
File Name:	

Security System Layout



1 TOP TIER PLAN

Garahy Parking Garage

No#	Revision Description
1	Initial drafts completed

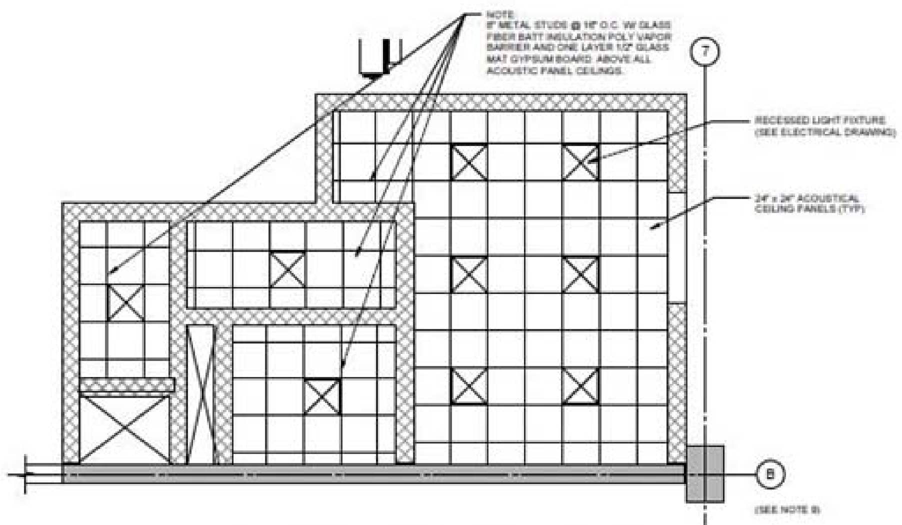
SYM	DESCRIPTION
ECB	EMERGENCY CALL BOX
○n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE
PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

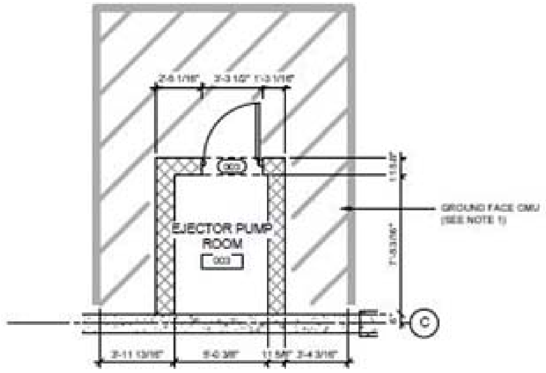
Engineered by:	
Drawn by:	
Scale: Not Applicable	
Job Number:	
Date:	
File Name:	

Security System Layout


NOTE:
8" METAL STUDS @ 16" O.C. W/ GLASS FIBER BATT INSULATION POLY VAPOR BARRIER AND ONE LAYER 1/2" GLASS MAT GYPSUM BOARD ABOVE ALL ACOUSTIC PANEL CEILINGS.
RECESSED LIGHT FIXTURE (SEE ELECTRICAL DRAWING)
24" x 24" ACOUSTICAL CEILING PANELS (TYP)
7
B
(SEE NOTE 9)

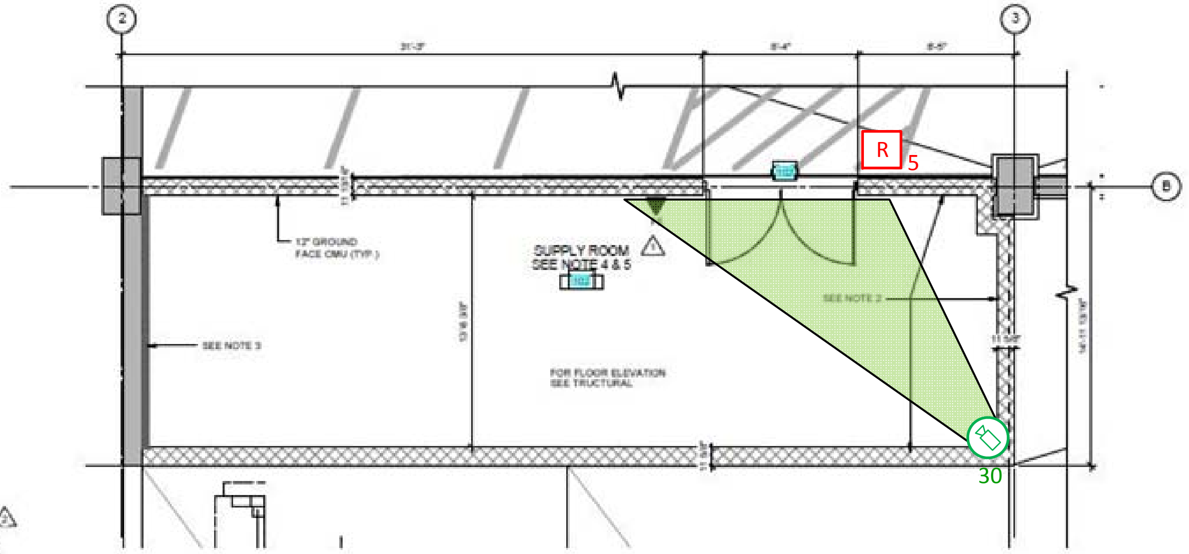
4 PARKING OFFICE REFLECTED CEILING

1/4" = 1'-0"



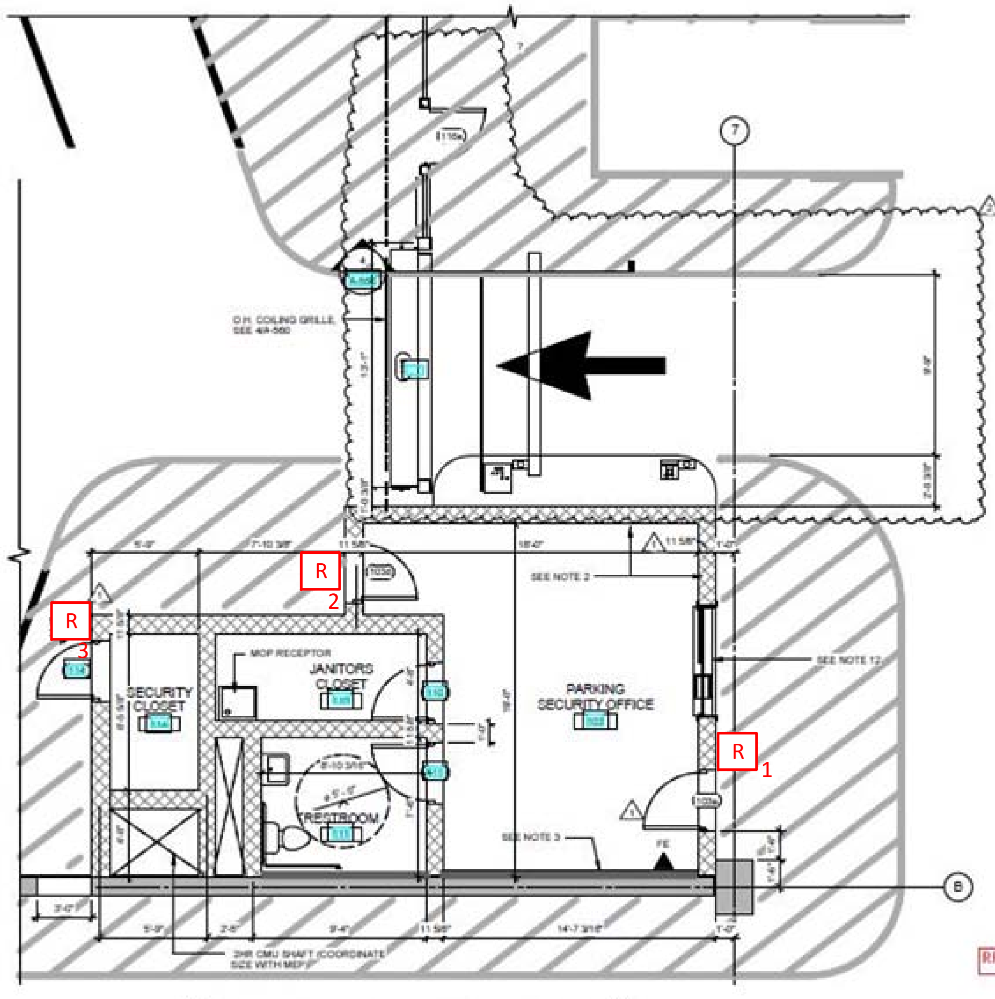
5 EJECTOR PUMP ROOM AT B1 TIER

1/4" = 1'-0"


2
3
B
R
5
SUPPLY ROOM SEE NOTE 4 & 5
12" GROUND FACE CMU (TYP.)
SEE NOTE 3
SEE NOTE 2
FOR FLOOR ELEVATION SEE TRUCTURAL
30

2 SUPPLY ENLARGED PLAN

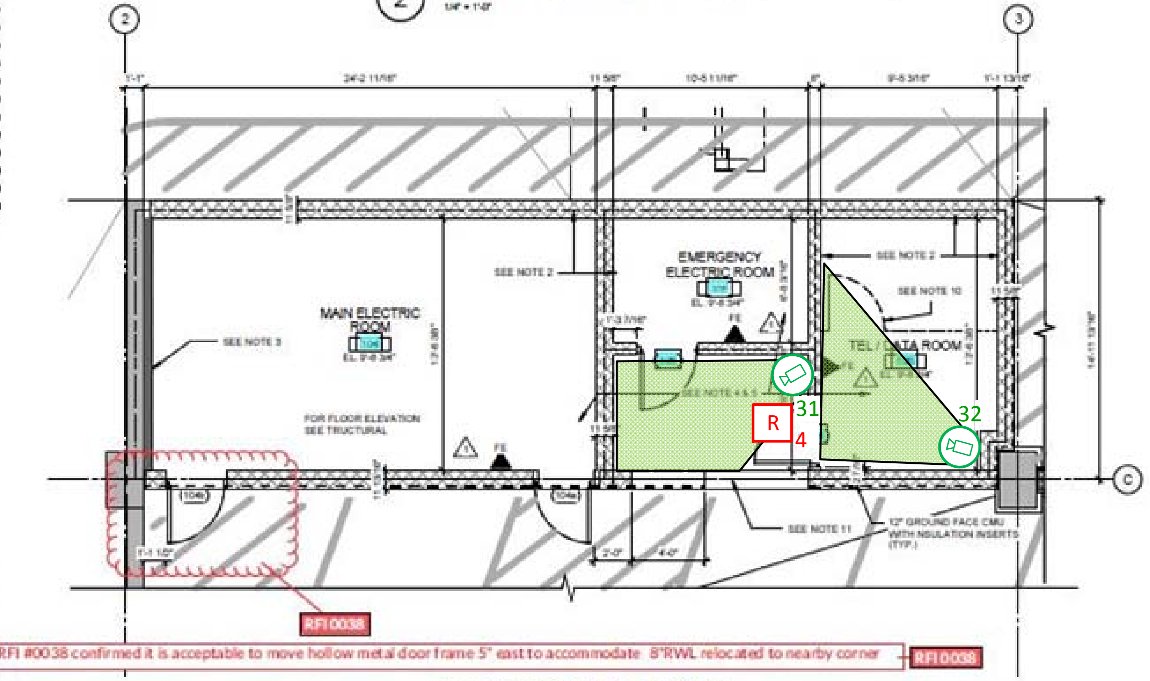
1/4" = 1'-0"



NOTE:
12" INSULATE GROUND FACE CMU AT ALL WALLS OF OFFICE ROOMS IN THIS PLAN

3 PARKING SECURITY OFFICE ENLARGED PLAN

1/4" = 1'-0"



RFI #0038 confirmed it is acceptable to move hollow metal door frame 5" east to accommodate 8"RWL relocated to nearby corner RFI 0038

1 ELECTRIC & TEL/DATA ENLARGED PLAN

1/4" = 1'-0"

Garahy Parking Garage

No#	Revision Description
1	Initial drafts completed

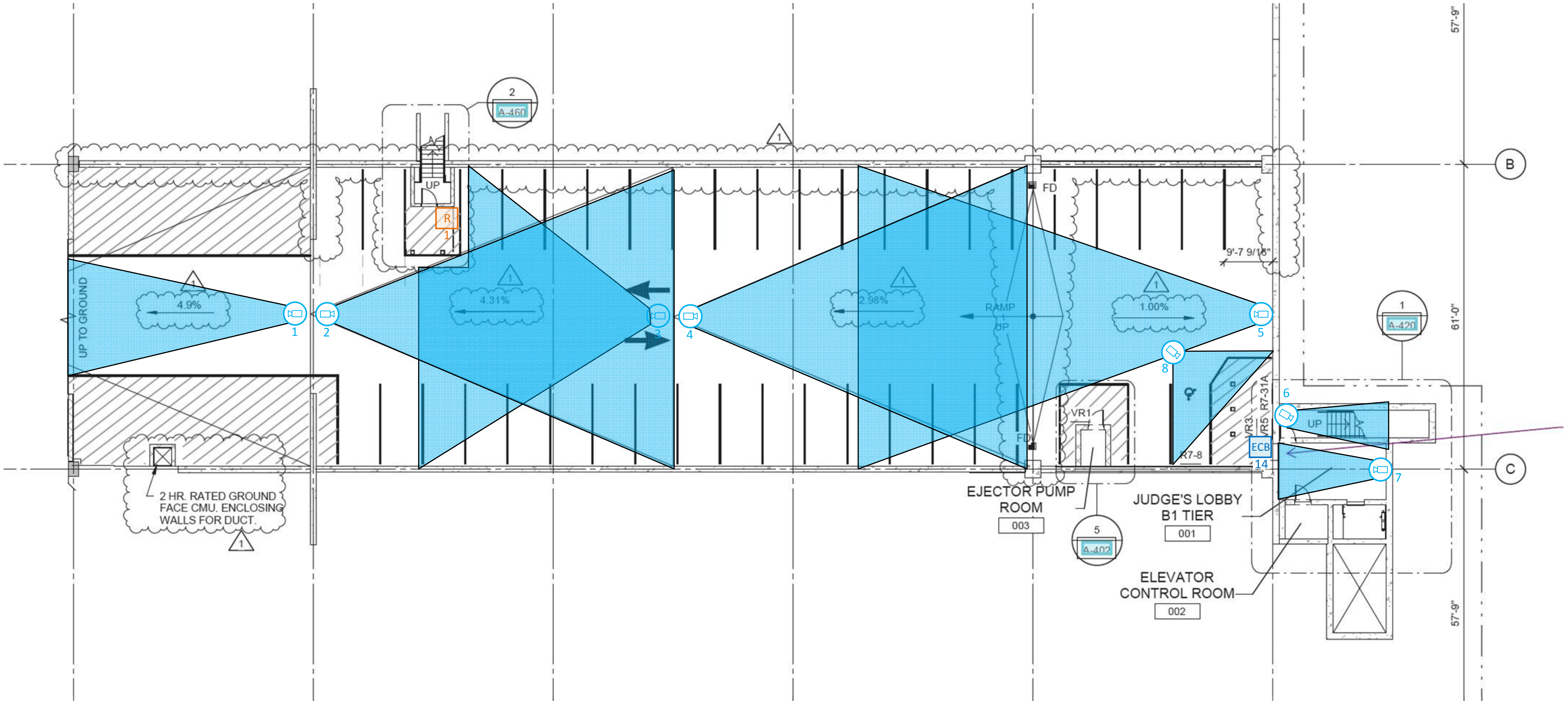
SYM	DESCRIPTION
ECB	EMERGENCY CALL BOX
○ n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

Engineered by:	
Drawn by:	
Scale: Not Applicable	
Job Number:	
Date:	
File Name:	

Security System Layout



1 B1 TIER PLAN

Garahy Parking Garage

No#	Revision Description
1	Initial drafts completed

SYM	DESCRIPTION
ECB	EMERGENCY CALL BOX
◯n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE
PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

Engineered by:	
Drawn by:	
Scale: Not Applicable	
Job Number:	
Date:	
File Name:	

Security System Layout

Security System Cable Types:

▭	○	Security Cameras - Category 6 - NFPA 70, Type CMP - Color: Green - Windy City Wire Model Number 5566060
WR	R	Access Control Cable: Door: Card Reader / Request to Exit / Door Contact / Lock (<300') - NFPA 70, Type CMP - Color: Yellow - Windy City Wire Model Number 4461030
WR	R	Access Control Cable: Door: Card Reader / Request to Exit / Door Contact / Lock (300'-500') - Color: Yellow - Windy City Wire Model Number 44 4466060IFS-50061030
DC	DR	Intrusion Detection Cable: Window Contact: 22/2 - NFPA 70, Type CMP - Color: Yellow - Windy City Wire Model Number 0043630
GB		Glass-Break Detector Cable: 22/4 - NFPA 70, Type CMP - Color: Yellow - Windy City Wire Model Number 0043830
ICM	IC	Intercom: Power: NFPA 70, Type CMP - Color: Yellow - Windy City Wire Model Number 0023630, Door Unlock: NFPA 70, Type CMP - Color: Yellow - Windy City Wire Model Number 0023630, Communications: NFPA 70, Type CMP - Color: Green - Windy City Wire Model Number 5566060

Toyota Research Institute
4440 El Camino Real
Los Altos, CA 94022

No#	Revision Description
1	Initial drafts completed

SYM	DESCRIPTION
Rn	CARD READER
○n	DOME HIGH DEF. CAMERA
DC 8	DOOR CONTACT
DR	DOOR RELEASE

GARRAHY COURTHOUSE
PARKING GARAGE
PROVIDENCE, RI

GSC
CONSULTING

Engineered by:
Drawn by:
Scale: Not Applicable
Job Number:
Date:
File Name:

Security System Layout