SECTION 28 05 00 - ELECTRONIC SECURITY COMMON WORK

1.01: Reference to Owner's General Conditions

A. The Owner's General Conditions shall be considered part of this Specification Section, as applicable. Unless this Section contains statements, which are more definitive or more restrictive than those contained in the General Conditions, this Specification shall not be interpreted as waiving or overruling any requirements expressed in the General Conditions.

B. To the fullest extent permitted by law, the Contractor shall indemnify and hold harmless the Owner, Architect, Consultant, and agents and employees of any of them from and against claims, damages, losses, and expenses. This shall include, but not be limited to, attorney's fees arising out of or resulting from performance of the Work, provided that such claim, damage, loss or expense is attributable to bodily injury, sickness, disease or death, or to injury to or destruction of tangible property (other than the Work itself) including loss of use resulting there from, but only to the extent caused in whole or in part by negligent acts or omissions of the Contractor, a Subcontractor, anyone directly or indirectly employed by them or anyone for whose acts they may be liable, regardless of whether or not such claim, damage, loss or expense is caused in part by a party indemnified hereunder. Such obligation shall not be construed to negate, abridge, or reduce other rights or obligations of indemnity which would otherwise exist as to a party or person described in this paragraph.

1.02: Definitions

A. The following shall serve as general identifiers as specified herein.
   1. Owner – The Owner is the Hyatt Regency. "Owner" shall refer to the actual Owner and/or their designated representative(s).
   2. Consultant – The Consultant is Guidepost Solutions.
   3. Contractor – The Contractor is the firm submitting a proposal (bid) to furnish and install the Work as defined within this Specification. This firm may also be referred to as the Security Contractor.
   4. Project – The Project is the Electronic Security System installation for the Hyatt Place, at South Gate DFW, TX.
   5. Work – The term "Work" means all construction and services specified within this document and as indicated on the Drawings. The Work includes all related labor, materials, equipment, and services provided, or to be provided, by the Contractor to fulfill the proposal's obligations.

B. Drawings – The term "Drawings" means all Security System Drawings and associated sketches, details, riser diagrams, etc.

C. As used in the Drawings and Specifications for the Work, certain non-technical words and phrases shall be understood to have specific meanings as follows, regardless of indications to the contrary in the General Conditions or other documents governing the Work.
   1. "Furnish" – Purchase and deliver to the project site complete with every necessary appurtenance and support, all as part of the Security Systems Work. Purchasing shall include payment of all sales taxes and other surcharges as may be required to assure that purchased items are free of all liens, claims, or encumbrances.
   2. "Install" – Unload at the delivery point at the site and perform every operation necessary to establish secure mounting and correct operation at the proper location in the project, all as part of the Work.
   3. "New" – Manufactured within the past year and never before used.

4. "Provide" – Furnish and Install.

D. Regardless of their usage in codes or other industry standards, certain words or phrases as used in the Drawings or Specifications for the Work, shall be understood to have the specific meanings as ascribed to them in the following list:

1. "ACAMS" – Access Control and Alarm Monitoring System.
2. "Circuit" – Any specific run of circuitry.
3. "Circuitry" – Any Work which consists of wires, cables, raceways, and/or specialty wiring method assemblies complete with associated junction boxes, pull boxes, outlet boxes, joints, couplings, splices, and connections except where limited to a lesser meaning by specific description.
4. "Concealed" (as applied to circuitry) – Covered completely by building materials, except for penetrations (by boxes and fittings) to a level flush with the surface as necessitated by functional or specified accessibility requirements.
5. "DGP" – Data Gathering Panel.
6. "Exposed" (as applied to circuitry) – Not covered in any way by building materials.
7. "Normal Work Conditions" – Locations within building confines that are not damp, wet, or hazardous and that are not used for air handling.
8. "Patch Panel" – A System of terminal blocks, patch cords, and backboards that facilitate administration of cross-connecting cables.
9. "Raceway" – Any pipe, duct, extended enclosure, or conduit (as specified for a particular System) which is used to contain wires and which is of such nature as to require that the wires be installed by a "pulling in" procedure.
10. "Riser" – Shall refer to the portion of the installation that transmits between building floors (or between security System rooms), also referred to as "Backbone Cabling".
11. "Security Closet" – The enclosed area or room specifically designated for the routing, termination, and/or cross connecting of security System cable (i.e. riser cable) to other security System cable and/or equipment.
12. "SMS" – Security Management System, includes all components contained herein that work in conjunction to create and completely integrated and fully functioning system as described within the Drawings and Specifications.
13. "Security System Wiring" – see "Circuitry".
14. "Security System Work" – See "Work".
15. "Standard" (as applied to wiring devices) – Not of a separately designated individual type.
16. "Subject to Mechanical Damage" – Exposed within seven (7) feet of the floor in mechanical rooms, manufacturing spaces, vehicular spaces, or other spaces where heavy items are moved around or rigged as a common practice or as required for replacement purposes.
17. "System" – See "SMS".
18. "TBD" – To be determined.
19. "Wiring" – see "Circuitry".
20. "Workstation" – The location where security System monitoring equipment is provided.

E. Where the word "conduit" is used without specific reference to type, it shall be understood to mean "raceway".

F. Reference to "U.L. (Materials Construction) Standards" shall mean the "Standards for Safety" published by Underwriters Laboratories, Inc.

G. Reference to "NEMA Standards" shall mean the "Approved Standards" published by the National Electrical Manufacturers Association.

H. Reference to "ANSI Standards" shall mean the standards published by the American National Standards Institute.

I. Reference to "IEEE Standards" shall mean the standards published by the Institute of Electrical and Electronics Engineers.

J. Reference to "BICSI Standards" shall mean the guidelines and methods published by the Building Industries Consulting Service International.

1.03: Scope of Work

A. The Work shall include installation and commissioning of the following:
   1. Integrated Security Management System (SMS) consisting of:
      a. Access Control and Alarm Monitoring System (ACAMS)
      b. Video Surveillance System (or Closed Circuit Television System, CCTV)
      c. Network Switches (NS) and Security Network
      d. Uninterruptible Power System (UPS)
   2. Interfaces:
      a. SMS/ACAMS
      b. SMS/CCTV
      c. SMS/NS
      d. SMS/UPS
   3. Miscellaneous:
      a. Wire and cable to install all equipment as specified herein.
      b. Conduit and back boxes (not shown on the Drawings as provided, but required for a complete installation).
      c. Equipment Racks and Enclosures required to house all equipment as specified herein.

B. The Work detailed within the Contract Documents has been specified to meet certain requirements for performance, appearance, and costs. Some information, such as exact locations of field equipment, exact wire routing, and exact conduit requirements have been intentionally omitted. It shall be the responsibility of the Contractor to implement the guidelines and requirements contained in the Contract Documents and translate them into a complete design package containing all elements necessary for a complete, operational, and functionally integrated Security System.

C. Provide all work as detailed in the Contract Documents as a turnkey installation including all material, labor, warranties, taxes, freight, and permits. Only items and requirements specifically stated to be provided by others shall not be a requirement for this Section of the Work.

D. Coordinated Work
   1. Coordinate with related trades to schedule the Work and ensure a complete installation in accordance with the schedule outlined by the Owner.

2. Within the Contract Documents, certain mounting heights and general device locations are specified. Carefully examine existing conditions to coordinate final equipment/device locations, facility designations, floor accessibility, floor type, ceiling heights, ceiling accessibility, and ceiling types. Verify the exact mounting locations and mounting heights of all equipment with the Owner prior to installation. Notify the Owner in the event that a particular location appears to be unsuitable.

3. Coordination with Property Management Team

   a. During demolition and construction phases, Contractor shall fully coordinate with the Property Management team prior to any disruption of operation to critical equipment (mechanical, plumbing, electrical, fire alarm, telecommunications, security, etc).
   b. During demolition and construction phases, if disruption occurs to other tenant's systems that affect normal daily operations, Contractor shall immediately contact the Property Management team.

1.04: Related Sections

1. Division 01 - General Requirements
2. Division 08 - Openings (Door Hardware)
3. Division 11 - Equipment
4. Division 26 - Electrical
5. Division 27 – Communications
6. 28 10 00 – Electronic Access Control and Intrusion Detection
7. 28 23 00 - Electronic Video Surveillance

1.05: General Conditions

A. The Contractor represents that they are familiar with, and have expertise in the Work of this nature and scope. The Contractor further agrees that they shall provide all Work as may be required to make a complete job of that which may not be fully defined in the Contract Documents.

B. The Contractor shall comply with all of the regulations, including OSHA safety regulations of municipal, city, local, and other government agencies having jurisdiction concerning the work of the Contractor. The Contractor shall give all notices and comply with all laws, ordinances, codes, rules, and regulations bearing on the conduct of the Work. If the Contractor performs any work, which is contrary to such laws, ordinances, codes, rules and regulations, they shall make all changes for compliance and bear all associated costs.

C. The Contractor shall be responsible to provide and maintain a storage facility. If this storage facility is required to be on-site it shall be the Contractor's responsibility to coordinate the size and spatial requirements with the Owner. The Contractor shall assume full responsibility for the storage facility and all contents, unless otherwise indicated by the Owner.

D. The Contractor shall utilize good housekeeping practice with respect to their work including cleanup of all dirt and debris created by the Contractor during installation operations on a daily basis.

E. The Contractor shall provide all protection necessary to safeguard their work from damage by their operations and the operations of others. Unless the Contractor proves to the Owner's satisfaction that the Work has been damaged by others, the Contractor shall promptly repair, adjust, and clean all defective installations and bear all associated costs.

F. All of the Contractor's work shall be tested and inspected by all authorities having jurisdiction and in accordance with all Specifications. The Contractor shall coordinate and cooperate fully and shall provide at no additional cost to the Owner, manpower, blueprints, facilities, scaffolds, etc. to reasonably assist the inspectors.

G. The Drawings are, in general, diagrammatic. The Contractor shall coordinate the installation of all devices and/or equipment with the Owner prior to installation based on the existing field conditions.

H. The Contractor shall examine the site and the Contract Documents and review with the Owner the designated areas of access, delivery, and storage for the Contractor's use. The Contractor agrees that such areas are satisfactory and sufficient for their needs in the completion of their work and in conformance with the terms of this Contract.

I. Should any questions of union jurisdiction arise, the Contractor shall immediately take steps to settle such disputes and shall use such labor as may be determined to have jurisdiction, at no additional cost to the Owner. Should the Contractor fail to take expeditious action, they shall be responsible for any time lost because of delays arising from such a dispute.

J. The Owner reserves the right to furnish any materials necessary for the Project.

K. All permits required for any part of the Contractor's work shall be procured and paid for by the Contractor. The Contractor shall determine all permits required and transmit this information to the Owner.

L. The Contractor warrants that both they and their subcontractors are licensed as required by the authorities having jurisdiction and as required by local ordinances.

M. The Contractor shall state if they intend to utilize a subcontractor, and provide said subcontractor's name and address. The subcontractor shall comply with all the same rules, regulations, laws, codes, licenses, etc. as required by the Contractor and as specified herein. The Owner reserves the right to approve or disapprove any subcontractor proposed by Contractor.

N. The Architect shall provide to the Contractor all available AutoCAD backgrounds for related floor plans for the facilities. All pre-fabrication and record drawings required for the Project and as stated herein, shall be completed within the latest version of AutoCAD.

O. The Contractor, upon receiving notice from Owner that the Contractor has furnished inferior, improper or unsound work or materials (including equipment), or work or materials at variance with that which is specified, will, within 24 hours, proceed to remove such work or materials and make good all other work or materials damaged thereby, and, at the option of the Owner, the Contractor shall immediately replace such work or materials with work or materials as specified. The removal, replacement, and repair shall be performed at such times and with manpower sufficient, in the judgment of the Owner, so as to avoid disturbance to occupants, or other ongoing work for the Project.

1. If the Contractor does not remove such unsound Work within a reasonable time, the Owner may remove it and may store the material at the expense of the Contractor. If the Contractor does not pay the expenses of such removal within ten (10) days' time thereafter, the Owner may, upon written notice, sell such materials at auction or at private sale and shall account for the net proceeds thereof, after deducting all the costs and expenses that should have been borne by the Contractor and all expenses of the sale.

2. The Owner shall have the authority at all times, until final completion and acceptance of the Work, to inspect and reject work and materials which in its judgment are not in conformity with the Drawings and Specifications, and its decision in regard to character

and value of Work shall be final and conclusive on both contracting parties. If the Owner permits said Work or materials to remain, the Owner shall be allowed the difference in value or shall at its election have the right to have said Work or materials repaired or replaced, as well as the damage caused thereby, at the expense of the Contractor, at any time within one (1) year after the completion of the entire project, or within such longer period as may be covered by any guaranty; and neither payments made to the Contractor, nor any other acts of the Owner, shall be construed as evidence of acceptance, waiver, or estoppel.

3. Any expense incurred by the Owner in connection with the foregoing, shall be borne by the Contractor, and the Owner may withhold money due to the Contractor or recover money already paid to the Contractor, to the extent of such expense.

P. It shall be understood that the Specifications and Drawings are complementary. Where there are conflicts between the Drawings and Specifications or within the Specifications or Drawings themselves, the overall design intent shall govern.

Q. To the extent that they govern the Work, the Specifications and Drawings also govern change order Work, if any.

R. The Drawings for the Work utilize symbols and schematic diagrams that have no dimensional significance. The Work shall be installed to fulfill the diagrammatic intent expressed on the Drawings, field layouts, and shop drawings of all trades.

S. Certain details appear on the Drawings for the Work that are specified with regard to the dimensioning and positioning of the Work. These are intended only for general information purposes. They do not obviate field coordination for individual items of the indicated Work.

T. Information as to general construction, architectural features and finishes, and structural build shall be derived from the existing conditions. Review existing conditions as necessary with the Owner.

U. Ratings of devices, materials, and equipment specified without reference to specific performance criteria shall be understood to be nominal or nameplate ratings established by means of industry standard procedures.

V. It is the intent of the Drawings and Specifications to provide a complete operating security System. All Work necessary to provide such a System shall be performed. Any discrepancies shall be brought to the attention of the Owner and the Consultant.

W. The Work called for under this Contract shall be carried on simultaneously with the Work of other trades and Owner functions in such a manner as to not delay the overall progress of the construction project. The Contractor is responsible for all coordination of the Work with other trades.

X. Include in the Work all necessary supervision and issuing of all coordination information to any other trades who are supplying work to accommodate the security System installation.

Y. For items of equipment which are to be installed but not purchased as part of the Work, the Work shall include:

1. Coordination of delivery
2. Unloading from delivery trucks
3. Safe handling and field storage up to the time of permanent placement in the project
4. Correction of any damage to the item(s)

5. Mounting in place and connection(s) as specified

Z. Items which are to be installed but not purchased as part of the Work shall be carefully examined upon delivery to the project. Claims that any of these items have been received in such condition that their installation will require procedures beyond the reasonable scope of the Work will be considered only if presented in writing within one (1) week of the date of delivery to the project of the items in question. The Work includes all procedures necessary to put in satisfactory operation all items for which no claims have been submitted as outlined above.

AA. Where cabling is specified to be provided by the Owner or his representative, the Contractor shall identify the cable types, quantities, and lengths required and provide them to the Owner to be ordered. It is the Contractor's responsibility to ensure that the information is complete and accurate. Any errors or omissions in the ordering information will be the responsibility of the Contractor.

1.06: Project Management

A. The Contractor shall provide a Project Manager to oversee and coordinate all activities on the Project

B. Project Manager's Duties and Responsibilities:

1. The Contractor shall provide to the Owner, as a part of the prefabrication submittal, the name of the Project Manager that will provide all duties and responsibilities as specified herein, during the term of the project.

2. The Project Manager shall maintain the ability of making all managerial decisions on behalf of the Contractor on a day-to-day basis, and shall retain the authority of accepting notices of deduction, inspection reports, payment schedules and any other project related correspondence on behalf of the Owner.

3. The Project Manager shall schedule and attend project management meetings, during which time all System related issues are discussed, scheduled, confirmed, and/or resolved.

4. The Project Manager shall be available during normal business hours (8:00 AM to 5:00 PM) within two (2) hours by telephone during the term of the project.

   a. After normal business hours, the Project Manager shall be available within four (4) hours by telephone during the term of the project.
   b. In the event that the Project Manager is not available within the allotted time frame, the Contractor may designate another employee to temporarily act as the Project Manager in all correspondence with the Owner.
   c. The Contractor shall ensure that any individual temporarily assuming the duties of the Project Manager is at equal or higher level in the Contractor's managerial chain of command.

5. Upon notification by the Owner, of any project related installation issue, or issue that may contradict the Specifications as stated herein, the Project Manager shall respond to such issue, verbally and/or in writing within an eight (8) hour period

   a. Responses to such issues as stated above shall include a clear understanding of the issue, along with a tentative plan of action, reflecting milestones and/or deadlines to resolve the issue.
   b. Where appropriate, based on the overall importance of the project issue, the Project Manager shall follow-up their initial response with a written response to the issue within 24 hours of identification of the issue.

6. Prior to the initiation of the Work, the Project Manager shall submit a schedule reflecting key milestones of the Work, including but not limited to the following:

a. Bid award
b. Kick-off meeting
c. Prefabrication submittal
d. Ordering, delivery, and installation of head-end System equipment
e. Field equipment delivery
f. Project management schedule
g. Payment schedule
h. Installation completion date
i. System training
j. Delivery of As-Built documentation
k. Delivery of Operations & Maintenance Manuals
l. Final System test
m. Acceptance of System

7. The Project Manager shall update the schedule on a weekly basis to reflect the status of each key milestone as the Work progresses.

8. As the System installation progresses, the Project Manager shall be capable of discussing any/or all of the above mentioned items at the request of the Owner, and shall address each item, as it relates to the current status of the Work.

1.07: Special Confidentiality Requirement

A. The Work is critical to the security of the Owner's facility. All Drawings, Specifications and other material and information about the Work are confidential information and shall remain secure and confidential at all times. Confidential information shall not be deliberately or inadvertently disclosed to anyone other than the Contractor's personnel and subcontractors who require disclosure to perform their portion of the Work.

B. The Contractor shall keep track of all confidential information at all times and shall ensure that all copies are accounted for at all times. The Contractor shall not permit any persons to have access to the confidential information of the Work unless and until the Contractor has assured itself of the trustworthiness of such persons.

1.08: References

A. The Security System, Network Equipment, and Cabling shall be installed in accordance with the latest applicable revisions pertaining to all applicable national, state, and local codes and standards including, but not limited to the following:

1. Uniform Building Code, (UBC)
2. Building Officials & Code Administrators International, Inc. (BOCA) National Building Code
3. Americans with Disabilities Act (ADA)
4. National Electrical Code (NEC)
5. Telecommunications Industry Association (TIA)
6. Electronic Industries Alliance (EIA)
7. American National Standards Institute (ANSI)
8. Underwriters Laboratories (UL) Applicable Standards for Safety
9. Underwriters Laboratories (UL) Applicable Standards for Proprietary Security Systems
10. National Fire Protection Association, (NFPA 70)

11. National Fire Protection Association Life Safety Code, (NFPA 101)

12. Local Governing Authorities Having Jurisdiction

1.09: Pre-Fabrication Submittals

A. General Description and Requirements

1. Submit pre-fabrication submittals in accordance with the Owner's construction schedule.

2. Pre-fabrication submittals shall consist of product data, shop drawings, samples, and a detailed completion schedule. Partial submittals will not be accepted without prior written approval from the Owner.

3. Pre-fabrication submittals shall be furnished in electronic formats as defined within this Section and as defined by the General Conditions.

4. No portion of the Work shall commence nor shall any equipment be procured until the Owner has approved the pre-fabrication submittals in writing.

5. A letter of transmittal identifying the name of the Project, Contractor's name, date submitted for review, shall accompany pre-fabrication submittals and a list of items transmitted.

B. Product data required as part of the pre-fabrication submittal shall include the following:

1. Equipment schedules listing all System components, manufacturer, model number and the quantity of each

2. General functional descriptions for each System

3. Manufacturer's data specification sheets for all System components, including any warranty information (sheets containing more than one device or component model number shall be clearly marked to delineate items included in the Work)

4. A complete list of cable and wiring types, sizes, manufacturer, and model number

5. A complete list of finishes and sample graphics, including custom art work and custom graphics (if applicable)

6. List of parts inventory to provide manufacturer recommended service and maintenance of the Work

C. Shop Drawings shall include the following:

1. Floor plan drawings indicating device locations with device legends

2. System riser diagram with all devices, wire runs, and wire designations

3. Schematic block diagrams for each System showing all equipment, interconnects, data flow, etc.

4. Wiring diagrams for each subsystem defining the interconnection of all inputs and outputs for all equipment

5. Wiring diagram for fail-safe release of electric locking mechanical

6. Fabrication shop drawings for all custom equipment (if applicable)

7. Plans and elevations of the equipment racks quantifying all equipment to be mounted therein

8. Elevations of security closet layouts showing panel locations, power supply locations, conduit, wire ways, wire molds, and all other equipment

9. The Contractor shall submit samples of any equipment components upon request of the Owner.

10. Samples submitted shall be the latest version of equipment.

11. It is the responsibility of the Contractor to confirm all dimensions, quantities, and the coordination of materials and products supplied by the Contractor with other trades. Approval of shop drawings containing errors does not relieve the Contractor from making corrections at their expense.

1.010: Quality Assurance

A. Contractor Qualifications

1. Work specified herein shall be the responsibility of a single Contractor. Bid submission shall document a minimum of five (5) years experience in the fabrication, assembly, and installation of Systems of similar complexity as specified herein. The documentation shall include the names, locations, and points of contact for at least three (3) installations of the type and complexity specified herein.

2. The Contractor shall have local in-house engineering and project management capabilities consistent with the requirements of the Work.

3. By submitting a bid, the Contractor thereby certifies that it is qualified in all areas pertaining to, directly or indirectly, the Work. In the event the Contractor becomes unable to complete the Work in accordance with the Contract Documents, or the satisfaction of the Owner, it shall be the responsibility of the Contractor to retain the services of applicable manufacturers' representatives to expeditiously complete the Work in accordance with the Owner's construction schedule with no additional cost to the Owner.

4. The Contractor shall maintain, or establish and maintain, a fully staffed office including a service center capable of providing maintenance and service to the Project. The Contractor shall staff the service center with factory trained technicians and adequately equip the office to provide emergency service within four (4) hours after being called, 24 hours per day.

5. The Contractor shall provide factory-certified technicians to install, commission, and maintain the Work. All installing personnel shall be licensed as required by local and/or state jurisdictions.

6. The Contractor shall ensure compliance with, and have a thorough understanding of, all local codes and contract conditions pertaining to this Project.

7. The Contractor shall maintain an inventory of spare parts and other items critical to System operation and as necessary to meet the emergency service requirements of this Project within the local service center.

B. Product Standards

1. All equipment and materials for contained herein shall be the products of recognized manufacturers and shall be new.

2. New equipment and materials shall:

   a. Be Underwriters Laboratories, Inc. (U.L.) listed and approved where specifically called for; or where normally subject to such U.L. labeling and/or listing services.
   b. Be clearly labeled identifying make, model, and manufacturer.
   c. Be without blemish or defect.
   d. Be products that meet with the acceptance of the agency inspecting the security Systems work.

3. It is the intent of these specifications that wherever a manufacturer of a product is specified, and the terms "other approved" or "approved equal" are used, the substituted item shall conform in all respects to the specified item. Consideration will not be given to claims that the substituted item meets the performance requirements with lesser construction. Performance as delineated in schedules and in the specifications shall be interpreted as minimum performance.

4. Substituted equipment or optional equipment, where permitted and approved, shall conform to space requirements. Any substituted equipment that cannot meet space requirements, whether approved or not, shall be replaced at the Contractor's expense. Any modifications of related Systems as a result of substitutions shall be made at the Contractor's expense.

5. The approval of shop drawings, or other information submitted in accordance with the requirements hereinbefore specified, does not ensure that the Owner or Consultant attests to the dimensional accuracy, dimensional suitability of the material, or mechanical performance of equipment. Approval of shop drawings does not invalidate the Drawings and Specifications.

6. Substitutions of SMS equipment shown on the schedules or designated by model number in the specifications will not be considered if the item is not a regular catalogued item carried by the manufacturer.

7. Manufacturers Recommendations: Where installation procedures of any part thereof are required to be in accordance with the recommendations of the manufacturer of the material being installed, printed copies of these recommendations shall be furnished prior to installation. Installation of the item will not be allowed to proceed until the recommendations are received. Failure to furnish these recommendations may be cause for rejection of the material.

8. The Contractor shall provide a complete fit-out of the security closets for review by the Owner and Consultant prior to continuing with the installation of the other security closets. The closet fit-out shall include all cabinets, conduit, blocks, patch panels, frames, labels, etc.

9. Within the Specifications, certain manufacturers have been listed. These manufacturers are listed for example purposes (unless followed by "No Exceptions"). The Contractor may substitute manufacturers and models that may be more cost effective or readily available than that specified. However, all substitutions shall meet or exceed the specified functional and technical requirements. Acceptance of such substitutions is at the discretion of the Owner, and/or Consultant.

10. All exterior devices shall be sealed and protected against all weather conditions consistent with the region including heat, cold, moisture, dust, etc.

1.011: Warranty and Maintenance

A. Contractor shall provide a two (2) year warranty for the Work. The warranty shall cover all Work, Systems, and subsystems against defects in materials and workmanship. The Work as specified herein, including all materials and labor, but excepting any existing devices and equipment which are incorporated in the completed Work, shall be warranted to be free from defects in design, workmanship, and materials. Further, the Contractor shall warrant that the completed Systems, including all components (except those, which are existing or provided by others), are of sufficient size and capacity to fulfill the requirements of the Specifications.

B. The warranty shall be valid for a period of two (2) years following the date of System acceptance by the Owner. System acceptance shall commence when all parts, components, sub-Systems, and Systems have been tested, shown to be working in accordance with the Specification, and approved by the Owner.

C. Nothing contained in the Contract Documents shall be construed to establish a shorter period of limitation with respect to any other obligation, which the Contractor might have under the Contract Documents or any manufacturer's warranty. The establishment of the time period of two (2) years after the date of final acceptance of the Work or such longer period of time as may be prescribed by law or by the terms of any warranty required by the Contract Documents, relates only to the specific obligation of the Contractor to correct the Work, and has no relationship to the time within which its obligation to comply with the Contract Documents may be sought to be enforced, nor to the time within which proceedings may be commenced to establish the Contractor's liability with respect to its obligations other than specifically to correct the Work or equipment.

D. Warranty Service:

1. In the event that defects in the materials and/or workmanship are identified during the warranty period, the Contractor shall provide all labor and materials as may be required for prompt correction of the defect.

2. During the warranty period, the Contractor shall, upon receipt of a request for service form the Owner, deploy service personnel to the Owner's premises within four hours to initiate corrective action.

3. All warranty service and repair work shall be performed by personnel, who have been trained, certified and is experienced in the operation and maintenance of the installed System(s).

4. Unless otherwise requested by the Owner, warranty service shall be performed during normal business hours (8:00 AM to 5:00 PM), Monday through Friday, exclusive of Holidays. In the event that the Owner requests warranty service to be performed during other than normal business hours, the Contractor shall be compensated for such service at 150% of his normal hourly service rates as listed in the bid proposal for this project.

5. Warranty service shall include the replacement of all parts and/or components as required to restore normal System operation. In the event that System parts or components shall be removed for repair, it shall be the responsibility of the Contractor to furnish and install temporary parts and/or components as required to restore normal System operation until the repaired parts or components can be repaired and re-installed.

6. It shall be the responsibility of the Contractor to maintain an inventory of spare parts or to arrange for manufacturer parts support as required ensuring correction of all critical component failures or malfunctions within 48 hours of the Owner's request for service. Critical parts shall be defined as those, which govern or affect the normal operation of more than one field device.

7. The Contractor's warranty obligation shall include correction of any software/firmware defects, which may be identified during the warranty period. Any failure of the software/firmware to perform as specified by the software/firmware manufacturer at the time of final acceptance shall be defined as a software/firmware error.

8. In the event that the Contractor determines and successfully demonstrates to the Owner that service or repairs are required as a result of misuse, abuse, or abnormal wear and tear, the Contractor shall be compensated for such service or repairs at the Contractor's hourly rates as listed in the bid proposal for the Project. Similarly, such compensation to the Contractor shall apply in the event that repairs are required for devices and equipment not provided by the Contractor but incorporated in the completed Systems.

9. Immediately following the completion of a warranty repair or service call, the Contractor's service personnel shall submit a written report to the Owner which details the service work performed, the cause of the trouble, and any outstanding work which is required to restore complete and normal operation.

E. The Owner reserves the right to expand or add to the System during the warranty period using firm(s) other than the Contractor for such expansion without affecting the Contractor's responsibilities, provided that the expansion is done by a firm which is an authorized dealer or agent for the equipment or System being expanded.

F. The Contractor shall perform preventative maintenance during the warranty period as part of the warranty service. The Contractor shall submit a list of items to be included in the preventative maintenance program and the service to be performed. Preventative maintenance shall include, but not be limited to, the following.

1. Semi-Annual Preventive Maintenance

    a. Inspect, test, clean, and adjust UPS. Replace batteries as necessary.
    b. Inspect and clean all SMS control panels and components.
    c. Inspect, test, and clean power supplies. Replace batteries as necessary.
    d. Inspect, clean and vacuum all equipment racks.
    e. Inspect and clean the system file server, workstations, and printers. Perform hardware, firmware, software, and disk drive maintenance as required to ensure optimum performance.
    f. Run SMS diagnostics and perform file maintenance to insure optimal performance.
    g. Test and adjust all CCTV System pan, tilt, zoom, and preset functions. Inspect, clean, and adjust CCTV System CPUs, DVRs, and NVRs.
    h. Clean all camera housings.
    i. Visually observe all camera and monitor displays and adjust as needed for optimal performance.

G. Include a manufacturer's software maintenance agreement as part of the Warranty. This agreement shall include all software updates, revisions, telephone service assistance, and training for any changes in operation.

H. Provide written notice to the Owner documenting any Work performed during the warranty period, including any preventative maintenance Work performed.

I. Provide loaner equipment that is fully compatible with the SMS for any equipment not field repairable.

J. Loaner equipment for components that shall be shipped to/from the manufacturer or distributor shall be on site and operational within 48 hours of the component failure. Furnish lists of equipment that will require shipment from the manufacturer or distributor and lead times associated with that equipment.

K. Repair or Replacement Service

1. Repair or replacement service during the warranty period shall be performed in accordance with the following schedule:

    a. Schedule A: 7 days, 24 hours per day with a four (4) hour response time.
    b. Schedule B: 8:00 AM – 5:00 PM on business days, excluding holidays, with a four (4) hour response time.

2. Schedule A shall apply for major System components including, but not limited to, the file servers, System workstations, DVR/NVRs, and the uninterruptible power System.

3. Schedule B shall apply for all other components and devices.

4. As part of the proposal submission, the Contractor shall include a labor rate schedule for any warranty service required during hours not covered under schedule B.

L. Failure to Perform Service

1. Schedule A Components: The Contractor shall provide 14 days of additional total System warranty (at no additional cost to the Owner) for every two (2) consecutive days of System or device failure.

2. Schedule B Components: The Contractor shall provide seven (7) days of additional total System warranty (at no additional cost to the Owner) for every two (2) consecutive days of System or device failure.

M. If the Contractor is unable to restore System operation during the warranty period within two (2) business days of a System failure, the Owner reserves the right to require the Contractor to provide on-site manufacturer's service technicians at no cost to the Owner.

N. Provide on-line software maintenance and support during the warranty period including all software and hardware (including telephone modems as required). Modem access to the System shall be password protected and controlled by the Owner.

2.01: Uninterruptible Power Supply System

A. System Description
1. Where indicated on the Drawings, Contractor shall provide UPS system to back-up Security Systems head-end equipment. UPS equipment shall be rack mount type unit where possible, but may be free standing tower where appropriate.

2. Provide UPS units in equipment rooms and locations where required to sustain the operation of all security System equipment requiring AC power to remain functional. Including but not limited to SMS, ACAMS, and CCTV. Provide UPS units sized sufficiently to provide a minimum of 20 minutes of back-up power.

3. In the normal operating mode, the UPS units shall condition line power protecting against spikes, sags, surges, noise and other line problems.

B. Technical Specifications
1. Minimum Specifications:

a. On line operation: The UPS shall provide continuous, no break power during complete power loss or momentary interruption
b. Output protection: Current limiting
c. Input protection: DC fuse and battery charger fuse
d. Controls: On/off switch
e. Alarm contacts: UPS alarm and battery
f. Batteries: As required for 20 minute back-up of the required load

2. Acceptable Manufacturers:

a. American Power Conversion
b. Best Power Technology, Inc.
c. Controlled Power Company
d. Approved equal

2.02: Equipment Racks and Enclosures

A. Contractor may utilize available space in telecom equipment racks in IDF rooms. Coordinate all work and shared space in equipment racks with the Telecom Contractor and Owner.

B. Where sufficient space is not available in IDF equipment racks, Contractor shall provide new wall-mounted security equipment racks. New racks shall be of sufficient size to house all new equipment as specified and as required for the complete System installation. System equipment which shall be housed in equipment racks shall include, at a minimum:

1. Network Patch Panels
2. PoE Network Switches
3. Network Video Recorders
4. UPS Units

C. Functional Specifications
1. Where required, provide all equipment racks, enclosures, and associated equipment as required to accommodate all head end and monitoring equipment as shown on the Drawings and as specified herein.
2. Space in telecom equipment racks located in IDF may be utilized for the security System if available at appropriate locations, and if approved by the Owner.
3. Coordinate with the Owner to establish locations of equipment rack locations which will be required to house all of the head-end equipment for the security System.
4. Security Floor and Wall Equipment Racks
   a. Physically attach multiple rack sections.
   b. Provide the following minimum equipment and/or hardware for each equipment rack section:
      1) Power outlet strips in each rack. Power outlet strips shall provide spare outlets for future equipment.
      2) Solid top panels
      3) Sold side panels for each end of the equipment rack
      4) Blank panels for all rack space not occupied by equipment except where noted to be open
      5) Full height flush mounted rear doors with recessed handles and locks with ventilation louvers
      6) Lockable flush mounted smoked glass front doors
      7) Cable trays as required from the equipment racks to the wire ways, data gathering panels, and power supplies located within the Security Equipment Room
      8) Thermostatically controlled, filtered fans as necessary for adequate ventilation
      9) All rack mounting hardware, brackets, shelves, etc. as necessary to install all rack mounted equipment and devices.

D. Technical Specifications
1. Rack joints shall be welded; bolted joints shall not be acceptable.
2. All rack rails and mounting hardware shall be concealed.
3. All equipment racks and enclosures shall be keyed alike.
4. Acceptable manufacturers:
   a. Middle Atlantic
   b. Winsted
   c. Approved equal

2.03: Network Related Equipment

A. Refer to Specification Section 28 23 00 for requirements of the following:

1. PoE Network Switches (NS)
2. Network Patch Panels
3. Network Back-Bone Cabling

2.04: Wire and Cable

A. General Requirements:
1. Provide wire and cable as required to install the Security System as indicated on the Drawings and specified herein.
2. All wire and cable shall be Underwriter's Laboratories (UL) listed, and shall meet all national, state, and local code requirements for its application.
3. All wire and cable shall meet individual system or subsystem manufacturer Specifications.
4. All wire and cable shall be Plenum type cable and shall conform to the minimum requirements of Insulated Cable Engineers Association (ICEA) Standards.
5. Wire and cable shall comply with the applicable requirements of the National Electrical Code (NEC), latest edition, in regards to cable construction and usage.
6. The conductors of wires shall be copper, and have conductivity in accordance with the standardization rules of the Institute of Electrical and Electronics Engineers, Inc. (IEEE). The conductor and each strand shall be round and free of kinks and defects.
7. All cable carrying data or voice transmissions shall be shielded. All other cable shall be shielded where necessary for interference-free signals.
8. Insulation shall be rated for a minimum of 300V.
9. Color-coding shall be accomplished by using solidly colored insulation. Grounding conductors, where insulated, shall be colored solid green or identified with green color as required by the National Electric Code (NEC).
10. Protect copper conductor circuits of all exterior security devices against power surges with individual TVSS devices. Each transient voltage surge suppressor (TVSS) shall be UL listed, and shall be properly grounded per manufacturer's written recommendations.

B. Wire Types and Sizes
1. Signal Cable (Non-Power): Wire size shall be a minimum of 20 AWG, twisted, shielded, stranded, insulated, and jacketed.
2. Signal Cable (Low Voltage Power): Wire size shall be a minimum of 18 AWG, stranded, insulated, and jacketed.
    a. Wire size shall be a minimum of 18 AWG, twisted, stranded, insulated and jacketed and shall be used for cable runs less than 500 feet.
    b. Wire size shall be a minimum of 16 AWG, twisted, stranded, insulated and jacketed and shall be used for cable runs in excess of 500 feet, but less than 750 feet.
    c. Wire size shall be a minimum of 14 AWG, twisted, stranded, insulated and jacketed and shall be used for cable runs in excess of 750 feet, but less than 1,250 feet.
3. Security Camera Video Cabling
    a. IP Network Video Cabling

1) Shall be provided by the Telecom Contractor. Security Contractor shall coordinate all specific security related requirements with the Telecom Contractor.

2) Shall consist of (4) twisted pairs, 22-26 AWG.

3) Shall be Category 6 cabling (CAT 6).

4) Shall meet TIA/EIA standards for CAT6 cabling.

5) Shall be plenum rated cable.

6) Refer to Division-27 specifications.

4. Copper Network Cabling (including patch cables) for other security equipment

a. Contractor shall provide all required network patch cables within IDF and MDF rooms for complete security System network connectivity and functionality. Owner shall not have to provide any network patch cables to the Contractor.
   1) Shall consist of (4) twisted pairs, 22-26 AWG.
   2) Shall be Category 6 cabling (CAT 6).
   3) Shall meet TIA/EIA standards for CAT6 cabling.
   4) Acceptable Manufacturer's: AMP, or approved equal.
   5) All patch cables shall be blue.
   6) Patch cables shall be provided for uplink connection for security switches, NVR's, client workstations, digital video storage devices and other security equipment connected to the Owner's LAN.

b. Contractor shall provide (2) network patch cables for each IP camera, one at the camera location and one to patch from the Telecommunications Patch Panel to the Security Switch in IDF rooms.

5. Elevator Traveler Cable

a. All elevator traveler cabling required for security devices shall be provided and installed by the Elevator Contractor.
b. All elevator panel penetrations required for security devices shall be provided by the Elevator Contractor.
c. The Security Contractor shall coordinate the requirements of traveler cabling and security devices with the Elevator Contractor, GC, and Architect.
d. At a minimum, each elevator cab shall be provided with cable infrastructure for (1) Card Reader and (1) Fixed CCTV Camera, even if these devices are not indicated on the plans. This will accommodate future security devices if necessary.
e. Minimum Requirements:
   1) Card Reader: (1) 6-conductor 18 AWG (min) stranded cable with an overall braided shield and drain wire from the elevator car operating panel to the elevator machine room car controller. Provide 3' service loop at the car operating panel and sufficient length in the elevator machine room to reach the Security System Interface Panel, plus 4' service loop. Cable shall be unspliced.
   2) Fixed CCTV Camera: (1) RG-6/U CCTV coaxial cable and (1) 2-conductor 18 AWG (min) stranded cable with an overall braided shield and drain wire from the elevator car ceiling to the elevator machine room car controller. Provide 6' service loop at the car ceiling and sufficient length in the elevator machine room to reach the

Security System Interface Panel, plus 4' service loop. Cable shall be unspliced.

6. Acceptable Manufacturers: Belden, West Penn, or approved equal

3.01: Language Usage

A. English language shall be used throughout the security system, signage, labels, voice messages, instructions, manuals, software, and graphic displays.

3.02: Installation

A. Site Inspections

1. Continuously verify that the site conditions are in agreement with the Contract Documents and the design package. Submit a report to the Owner documenting changes to the site or conditions that affect the performance of the System to be installed. For those changes or conditions, which affect System installation or performance, provide (with the report) specification sheets, or written functional requirements to support the findings, and a cost estimate to correct the deficiency. No deficiency shall be corrected without written permission from the Owner.

2. Specific mounting locations, exact wire and cable runs, and conduit routing have not been specified or delineated on the Drawings. Coordinate all aspects of the Work with the Owner.

B. Coordination

1. Coordinate with the Owner to ensure that adequate conduit is provided and that equipment back-boxes are adequate for System installation.

2. Coordinate with the Owner to ensure that adequate power has been provided and properly located for the security System equipment.

3. Coordinate with the Owner to ensure that doors and doorframes are suitable to properly install electric locking hardware as required.

4. Coordinate locations of all devices with the Owner prior to installation.

5. Coordinate and verify the location of each piece of rack-mounted equipment with the Owner.

6. Coordinate custom SMS report requirements with the Owner. Submit report formats to the Owner for review and acceptance.

7. Coordinate database setup with the Owner prior to initial programming of the security systems prior to data entry.

8. Coordinate final camera locations, heights, desired views, and camera mount requirements with the Owner prior to installation.

9. Coordinate finishes and colors of all equipment with the Owner. Submit all finish and graphics for all equipment in public areas to the Owner for approval prior to installation.

C. General

1. Verify acceptance of each type of specified request-to-exit hardware for each application with local life safety code officials.

2. Verify fail-safe and fail-secure lock requirements with the Owner.

3. Contractor or equipment manufacturer logos or names shall not be visible on equipment in public areas.

4. Provide tamper proof fasteners for all equipment in public areas. Fastener finish shall match equipment finish.

D. Equipment: Provide equipment as indicated on the Drawings and specified herein. Additional specific installation requirements are as follows:

1. Security Equipment Room and DGP Locations

   a. Configure security equipment as indicated in the Drawings.
   b. Wire all power supply power fail alarm contacts in each equipment room as a single alarm input to the SMS.
   c. Wire each power supply low battery alarm contact as individual alarm inputs to the SMS.

2. DGPs

   a. Configure the System such that devices can be connected to spare input points, output points and card reader inputs on the DGP without requiring reconfiguration of the SMS.

3. Card Readers

   a. Wire card reader LEDs to indicate valid and invalid card reads, and door locked and unlocked conditions. All card reader LED indicators shall operate identically.

4. Electric Locking Mechanisms

   a. Interface with electric locking mechanisms provided by the door hardware supplier.
   b. Wire electric locking mechanisms as indicated on the Drawings.
   c. Wire fail-safe electric locking mechanisms in accordance with local codes.
   d. Wire fail-secure electric locking mechanisms and power supplies such that a fire alarm condition or building power failure shall not affect operation of the lock.

5. Delayed Egress Locking Devices

   a. Interface with delayed egress locking devices provided by the door hardware supplier.
   b. Wire delayed egress locking devices as indicated on the Drawings.
   c. Wire delayed egress locking devices for fail-safe operation in accordance with local codes.
   d. Interface with a normally closed alarm contacts that shall open upon activation of the unlock timer.
   e. Interface with sounder bypass control contacts. Wire SMS control output contacts to bypass sounder by System Workstation.
   f. Interface with lock control contacts activated by System Workstation and/or time schedule. Wire SMS control output contacts to lock/unlock devices by time schedule and/or System Workstation.

6. Fire Alarm Interface

   a. Connect (hard wire) fail-safe electric and time delay locking mechanical to the building fire alarm System for fail-safe release upon any fire alarm.
   b. Interface with a single low voltage/low current normally closed dry contact from the fire alarm System provided by the fire alarm contractor in the Fire Command Center (FCC). The contact shall open on any fire alarm condition.
   c. Provide all additional UL listed fail-safe relays and power supplies necessary to interface to this contact and unlock all fail-safe doors.

d. Connect fail-safe relays and power supplies to standard building power. Connection of fail-safe devices to emergency or UPS power shall not be acceptable.
e. Reference the Drawings for fire alarm interface requirements.

7. CCTV Cameras

a. Field verify the exact location and positioning of all cameras with the Owner prior to installation.
b. Provide distribution amplifiers or use looping video outputs to distribute a single video signal to multiple video devices (DVRs, NVRs, CPUs, monitors, etc.).
c. Provide ground isolation transformers as required to eliminate humbars and ground loops.
d. Power all cameras from centrally located power supplies in the Security Equipment Room and each DGP location.
e. Field verify and confirm views with the Owner prior to final installation and adjust camera positions and lens sizes as required.
f. Synchronize each camera to ensure roll-free switching. Use an oscilloscope as necessary to ensure precise synchronization of all CCTV Cameras.

E. System Programming and Data Entry

1. Provide all initial System programming and setup of the SMS including, but not limited to the following:

a. Graphical Maps and Icons: Coordinate with the Architect to obtain AutoCAD architectural backgrounds for implementation as graphical maps. Import all AutoCAD background information provided by the Architect and produce a complete set of graphical maps depicting all SMS points.
b. SMS Card Reader Information: Coordinate all card reader values and text, including descriptors, alarm messages, CCTV Camera call up, map call-up, and identification with the Owner.
c. Input and Output Points: Coordinate all input and output priorities and text, including descriptors, alarm messages, CCTV Camera call up, and map call up and identification with the Owner.
d. Initial CCTV Camera call-up and alarm information for interface with the CCTV System. All ACAMS alarms and invalid card read events shall be communicated to the CCTV System and initiate camera call-up and increased record frame rate of video for associated CCTV cameras. Pre and post alarm video recoding shall also be initiated and provided for the above events.
e. Initial System Users and Levels of Access: This shall include the designation of an Owner's representative at the "Super User" level immediately upon SMS initialization.
f. Initial programming and set-up of all card reader and card holder security access-levels. Coordinate all security access level requirements with Owner.
g. All automatic lock/unlock schedules, system time zones, and final Sequence of Operations for access controlled doors shall be coordinated with the Owner, and programmed by the Contractor.

2. Provide all initial System programming and setup of the CCTV including, but not limited to the following:

a. On-screen alphanumeric identification of each CCTV Camera on each Monitor. Coordinate descriptors with the Owner prior to programming.
b. Video system programming to provide for the most efficient multiplexed recording allowable by the software.
c. Graphical Maps and Icons: Coordinate with the Architect to obtain AutoCAD architectural backgrounds for implementation as graphical maps. Import all

AutoCAD background information provided by the Architect and produce a complete set of graphical maps depicting all CCTV points.

d. Initial setup for the interface with the SMS. The interface shall provide for automatic CCTV Camera selection upon alarms within the SMS as defined in the Specification. All ACAMS alarms and invalid card read events shall be communicated to the CCTV System and initiate camera call-up and increased record frame rate of video for associated CCTV cameras. Pre and post alarm video recoding shall also be initiated and provided for the above events. Coordinate automatic CCTV Camera selection, real-time record initialization, and DVR/NVR record status alarm annunciation requirements with the Owner prior to programming.

e. Automatic selection of a CCTV Camera adjacent to a Card Reader upon an invalid card use. Coordinate automatic camera selection requirements with the Owner prior to System programming.

f.

3. Provide all initial System programming and setup of the UPS System including, but not limited to the following:

   a. Alphanumeric identification for each alarm point. Coordinate descriptors with the Owner prior to programming.
   b. Unattended shut-down interface with SMS.

4. Enter all data needed to make the Security System operational. Deliver the data to the Owner on data entry forms, utilizing data from the Contract Documents, Contractor's field surveys and all other pertinent information in the Contractor's possession required for complete installation of the database. Identify and request from the Owner any additional data needed to make the Security System fully operational and integrated. The completed forms shall be delivered to the Owner for review and approval at least 90 days prior to the Contractor's scheduled date.

3.03: Wiring Techniques

A. Furnish and install all SMS wire and cable with the exception of traveling cable for elevator control and monitoring.

B. Provide code compliant fire proofing techniques for all penetrations of fire rated partitions and slabs, where the penetrations are made by or used for installation of the SMS.

C. Coordinate the routing of wire and cable requiring isolation from power, radio frequency (RF), electromagnetic interference (EMI), telephone, etc. with the Owner.

D. Run all wire and cable continuous from device location to the final point of termination. No mid-run cable splices shall be allowed.

E. Where splicing and/or patching of coaxial cable are deemed necessary, it shall be accomplished through equalization and/or distribution amplifiers. Provide power for the amplifiers as required. The exact location of all equalization/distribution amplifiers (as applicable) shall be indicated on the Record Drawings.

F. Furnish and install all coaxial cable such that ample slack is supplied at the device terminating end of the cable to compensate for any final field modifications in camera location. The extra cable (approximately three meters) shall be bundled and wrapped.

G. At no time shall any coaxial cable be subjected to a bend less than a 150 mm radius.

H. Wire and cable within DGPs, power distribution cabinets and other security enclosures shall be neatly installed, completely terminated, pulled tight with slack removed and routed in such a way as to allow direct, unimpeded access to the equipment within the enclosure. All wire and cable shall be bundled and tied. Ties shall be similar to T&B TyRap cable ties.

I. Provide heat-shrink to insulate all wire splices and connections. The use of electrical tape for splices and connections shall not be acceptable.

J. Visually inspect all wire and cable for faulty insulation prior to installation.

K. Provide grommets and strain relief material where necessary to avoid abrasion of wire and excess tension on Wire and Cable.

L. Make connections with solder-less devices, mechanically and electrically secured in accordance with the manufacturers' recommendations. Wire nuts shall not be an acceptable means of connecting wire and cable.

M. Neatly bundle and wrap all horizontally run (above accessible ceilings and not within conduit) wire and cable at three-meter intervals. Provide supports as required. All supports shall be UL listed for the application.

N. All System wiring within vertical riser shafts (as required) shall be bundled, wrapped and tied to the structure at three-meter intervals in order to isolate it from other wire and cable within the shaft. Additionally, all wire and cable within the shaft shall be supported at least every two floors using Greenlee Slack Grips (Split Mesh Lace Closing) or approved equal. Provide all personnel and equipment necessary to install and support the cable. All equipment shall be UL listed for the application.

3.04: Conduit, Boxes, and Raceways

A. Electrical Contractor shall provide and install all conduit and wiremold as necessary for a complete System installation. Refer to the Drawings for additional specific requirements.

B. Security Contractor shall be responsible to coordinate all specific security system requirements with the Electrical Contractor.

C. Conduit shall be carefully installed, properly and adequately supported as required to comply with the requirements outlined herein and as required by the NEC to provide a neat, Workmanlike installation. Horizontal conduit runs shall be supported by clamps, pipe straps, special brackets, or heavy iron tie, tied to the black iron structural members supporting the ceiling. Fastening of conduit to masonry walls, floor or partitions require malleable pipe clips with screws and suitable expansion sleeves.

D. All conduit shall be cut accurately to measurements established at the building and shall be installed without springing or forcing.

E. All required inserts shall be drilled-in and all openings required through concrete or masonry shall be saw cut or core drilled with tools specifically designed for this purpose.

F. Swab out and remove all burrs from conduit before any wires are pulled. All connector ends shall be supplied with the appropriate protective bushings.

G. Provide fire stops where conduits penetrate fire rated walls and/or floors.

H. Coordinate all raceway installation with the Owner.

3.05: Power Requirements

A. Electrical Contractor shall provide 120VAC power circuits where required for the security Systems.

B. Security Contractor shall be responsible to coordinate all specific security system requirements with the Electrical Contractor.

C. Connect to the AC power circuits and provide UL listed power supplies and transformers to distribute low voltage power to the System components as required.

D. Provide hinged cover terminal cabinets with tamper switches for all power supplies, transformers, and power distribution terminal strips. Provide all conduit and wiring from the AC power facilities to the terminal cabinets.

E. Surge Protection
1. Provide protection against spikes, surges, noise, and other line problems for all System equipment and components.
2. Protect the copper conductor circuits of all exterior security devices against power surges.
3. Each transient voltage surge suppressor (TVSS) shall be UL listed, and shall be properly grounded per manufacturer's written recommendations.

3.06: Labeled Doors and Frames

A. In no instance shall any UL labeled door or frame be drilled, cut, penetrated, or modified in any way.

B. The Contractor shall be responsible for replacing any labeled door or frame that is modified without written approval from the Owner.

3.07: Labeling

A. Label all controls as necessary to agree with their function.

B. Mark all Wire and Cable in common at both ends using a permanent method such as self-laminating cable marking tape. The tags shall be attached to the wire and able nylon cable ties in an accessible location so that they can easily be read. Tags shall be installed when wire and cables are installed. Labeling shall agree with Record Documentation.

C. Place wire identification numbers at each end of the conductor involved by using sleeve type, heat shrinkable markers. The markers shall be installed so as to be readable from left to right or top to bottom.

D. Mark all connectors with common designations for mating connectors. The connector designations shall be indicated on the Record Drawings.

E. Coil all spare conductors in the device back-box, panel wire way, or top of panel where wire way is not provided. These conductors shall be neatly bundled and tagged.

3.08: Training

A. ACAMS

1. Once beneficial use of the ACAMS may be granted to the Owner, provide a minimum of 8 hours of ACAMS operator training and 8 hours of ACAMS administrative/database training, on site, to representatives of the Owner.

2. Training sessions shall be performed by a certified Representative of the ACAMS Manufacturer. All expenses inured for Manufacturer Representative training sessions shall be included in the Contractor's bid proposal, and will not be billable to the Owner.

3. Operator training shall include, but not be limited to the following:

   a. All operating System procedures
   b. System configuration
   c. Alarm acknowledgment, alarm response logging, and map graphics functionality.

4. Administrative training shall include, but not be limited to the following:

   a. All operating System procedures and configuration variables
   b. Database functions and setup
   c. Card holder input and deletion procedures
   d. Report generation
   e. Applications programs (as applicable)
   f. Map graphics generation and manipulation.

5. Record, label, and catalog all training on DVD. Provide the recordings to the Owner for future in-house training sessions and/or reviews. Furnish all temporary equipment necessary for recording all training sessions.

6. The Contractor shall be on call during the Warranty to answer any questions the Owner might have. Maintain time sheets verifying the total hours of training provided. The Owner reserves the right to use any excess training hours, not used by the time of System completion, for future training as requested by the Owner until the total number of training hours has been completed.

B. CCTV System

1. Once beneficial use of the CCTV System may be granted to the Owner, provide a minimum of 8 hours of CCTV System operator training and 8 hours of CCTV System administrative training, on site, to representatives of the Owner.

2. Training sessions shall be performed by a certified Representative of the CCTV Manufacturer. All expenses inured for Manufacturer Representative training sessions shall be included in the Contractor's bid proposal, and will not be billable to the Owner.

3. Operator training shall include, but not be limited to the following:

   a. System operation
   b. Manual and automatic camera call-up procedures
   c. DVR/NVR functionality

4. Administrative training shall include, but not be limited to the following:

   a. System operation and configuration variables
   b. Manual and automatic camera call-up procedures
   c. DVR/NVR set up, configuration variables, and functionality
   d. Video playback functionality

5. Record, label, and catalog all training on DVD. Provide the recordings to the Owner for future in-house training sessions and/or reviews. Furnish all temporary equipment necessary for recording all training sessions.

6. The Contractor shall be on call during the Warranty to answer any questions the Owner might have. Maintain time sheets verifying the total hours of training provided. The Owner reserves the right to use any excess training hours, not used by the time of System completion, for future training as requested by the Owner until the total number of training hours has been completed.

3.09: System Start-Up

A. The Work shall be complete and ready to operate prior to final acceptance.

B. Load the entire initial user database into all programmable Systems up to the day of beneficial use of the System. The Owner shall assist in establishing procedural guidelines and in defining terminology and conditions unique to the Owner's operation.

3.010: Substantial Completion

A. In order to qualify for the Owner's consideration of Substantial Completion, the Work shall, at a minimum, meet the following requirements:
   1. All alarm points, access control points, and CCTV cameras, shall be installed and fully operational.
   2. The UPS shall be installed and all Security Monitoring Room and Security Equipment Room equipment shall be connected to UPS power.
   3. The initial cardholder database shall be fully loaded into the SMS.
   4. All sub-System interfaces shall be complete and operational.
   5. All required operator training shall have been provided to the Owner and/or its representatives.

B. Substantial Completion shall NOT be construed as final acceptance of the Work.

3.011: System Acceptance

A. Final acceptance testing of the Work will be conducted by the Contractor and witnessed by the Owner and/or the Consultant.

B. Prior to any final acceptance testing, the Contractor shall submit two (2) sets of preliminary Record Drawings to the Owner. The preliminary Record Drawings are to be used by the Owner during the System final test.

C. The Contractor shall submit a report matrix indicating completion or delinquency for each item included in the Specification and all subsequent addenda and bulletins as part of the Work. Should work on any item be under way, but not yet fully complete, indicate the extent (or lack thereof) of completion to date, and the proposed date of completion.

D. Conduct a complete test of the entire System and provide the Owner with a written report on the results of that test. During the course of this test, place the integrated System in service and calibrate and test all equipment.

E. A Security System Readiness Checklist shall be drafted by the Contractor and submitted to the Owner and the Consultant for approval prior to use for System testing.

F. Fully complete a Security Systems Readiness Checklist prior to the test of the System. The checklist shall accompany the written certification to the Owner that the installed complete System has been calibrated, tested, and is fully functional as specified herein. All items within the

Readiness Checklist are required to be complete before a final inspection of the System. If for some reason the Contractor is unable to fully comply with any of the listed conditions, a written statement describing the exception is to be submitted with the checklist for review.

G. Following completion of the initial testing and correction of any noted deficiencies, conduct a five (5) day burn-in test. The intent of the burn-in test shall be to prove the System by placing it in near real operating conditions. During this period the System shall be fully functional and programmed such that all points, interfaces, controls, reports, messages, prompts, etc. can be exercised and validated. Record and correct any System anomaly, deficiency, or failure noted during this period. Scheduling of the final acceptance test shall be based on a review of the results of this burn-in test.

H. Deliver a report describing the results of functional tests, burn-in tests, diagnostics, calibrations, corrections, and repairs including written certification to the Owner that the installed complete System has been calibrated, tested, and are fully functional as specified herein.

I. Prior to the final acceptance test, coordinate with the Owner for security related construction clean-up requirements. Security equipment closets and similar areas should be free of accumulation of waste materials or rubbish caused by operations under the Contract. At completion of the Work, remove all waste materials, rubbish, the Contractor's and it's subcontractors' tools, construction equipment, machinery, and all surplus materials.

J. Upon written notification from the Contractor that the System is completely installed, integrated, and operational, and the burn-in testing completed, the Owner and Consultant will witness the final acceptance test of the entire System.

K. During the course of the final acceptance test, the Contractor shall be responsible for demonstrating that, without exception, the completed and integrated System complies with the contract requirements. All physical and functional requirements of the project shall be demonstrated and shown. This demonstration will begin by comparing "as built" conditions of the System to requirements outlined in the Specification, item by item. Following the Specification compliance review, all System head-end equipment will be evaluated.

L. In order to sufficiently demonstrate the System's functionality, the security officer on duty and his/her superior may be requested to perform certain daily operations inherent to the System.
   1. As all of these operations depend heavily on the training outlined within the Specification, the Contractor shall have completed all of the required training prior to initiation of the final acceptance test.

M. The functionality of the various interfaces between Systems will be tested. This testing will include, but not be limited to the following:
   1. Correct CCTV Camera call-up on certain alarms within the SMS
   2. Generation of alarms from related Systems failure
   3. Fire alarm system fail safe lock release
   4. Control of any externally controlled devices and/or database System(s)

N. Following the System head-end equipment and monitoring location review, the installation of all field devices will be inspected. Areas examined will include general neatness and quality of installations, complete functionality of each individual device, and mounting, back box and conduit requirements compliance.

O. All equipment shall be fully operational during testing procedures. The Contractor shall provide all personnel, equipment, and supplies necessary to perform all site testing. A minimum of two (2) employees familiar with the System for the final acceptance test shall be present during the

testing. One employee shall be responsible for monitoring and verifying alarms while the other will be required to demonstrate the function of each device. Supply at least two (2) two-way radios for use during the test. A manufacturer's representative may be present on site to answer any questions that may be beyond the technical capability of the Contractor's employees, if the Contractor so elects or by specific request of the Owner, at no charge to the Owner.

P. Upon successful completion of the final acceptance test (or subsequent punch list retest) the Consultant will issue a letter of recommendation that the Owner issue final acceptance of the System.

Q. The Owner and the Consultant retain the right to suspend and/or terminate testing at any time when the System fails to perform as specified. In the event that it becomes necessary to suspend the test, all of the Owner's fees and expenses related to the suspended test will be deducted from the Contractor's retainage. Furthermore, in the event it becomes necessary to suspend the test, the Contractor shall work diligently to complete/repair all outstanding items to the condition specified in the Specification and as indicated on the Drawings. The Contractor shall supply the Owner with a detailed completion schedule outlining phase-by-phase completion dates and a tentative date for a subsequent punch list retest. During the final acceptance test, no adjustments, repairs, or modifications to the System will be conducted without the permission of the Owner.

3.012: Record Documentation

A. Record Documentation shall include all information required in the Pre-fabrication Submittals but revised to reflect "as installed" conditions.

B. General Description and Requirements

1. Submit Record Documentation in accordance with the Owner's construction schedule.
2. Record Documentation shall consist of Record Drawings and Operation and Maintenance Manuals.
3. Provide a letter of transmittal with Record Documentation identifying the name of the Project, Contractor's name, date submitted for review, and a list of items transmitted.
4. Prior to the final acceptance of the Work, submit two draft sets of the Record Drawings portion of Record Documentation to the Owner. The draft copy shall be used during the final acceptance testing by the Owner.
5. Update all record documentation to reflect changes or modifications made during final acceptance testing as required and submit three blue/black lines and one reproducible set.
6. Upon completion of the Work, in addition to the above listed requirements, Contractor shall submit two (2) complete sets (2 hard copies and 2 electronic CD's) of the following documentation to the Property Management Team:
   a. As-built Record Drawings
   b. Complete Equipment List
   c. Operation and Maintenance Manuals
   d. Warranty Information

C. Record Drawings

Produce all Record" as-built" Drawings using the latest version of AutoCAD. Record drawings shall, at a minimum, include the following:

1. Floor plan drawings indicating device locations, with device legends indicating manufacturers and model numbers for each device

2. Floor plan drawings indicating wire routing, wire routing shall be delineated in straight line runs and be tagged with cable identification and terminal strip numbers to coincide with the installation

3. Mounting details for all equipment and hardware

4. Functional block diagrams for each subsystem
5. Wiring details showing rack elevations, equipment wiring and terminations, and inter-rack wiring

6. Wiring diagrams for all custom circuitry including interfaces to various control output controlled devices, i.e. overhead doors, automatic sliding doors, parking gate operators, fire alarm system interface, etc.

7. Wiring diagrams for each DGP, wiring diagrams shall be identical to those laminated and located with each DGP

8. Typical point-to-point wiring diagrams for each piece of equipment and groups of equipment within the System

9. Layout details for each riser location, including security panels, power supplies, junction boxes, conduit, and any other security related equipment

D. Operation and Maintenance Manuals
1. Operation and Maintenance (O&M) Manuals shall apply to all security related devices, equipment and software modules.

2. Operation and Maintenance Manuals shall be formatted as follows:

   a. Bind each manual in a hard-back loose-leaf binder.
   b. Identify each manual's contents on the cover.
   c. Provide a table of contents and tabulated sheets for each manual. Place tab sheets at the beginning of each chapter or section and at the beginning of each appendix if applicable.
   d. Any hardware manual demonstrating more than one model number of device on any one page shall be clearly marked as to delineate which model has been implemented in the Work.

3. Operation and Maintenance Manuals shall include, at a minimum, the following:

   a. Operational description of each subsystem
   b. Detailed programming descriptions for each subsystem
   c. Explanations of subsystem interrelationships
   d. Electrical schematics for each piece of equipment specified
   e. Power-up and power-down procedures for each subsystem
   f. Description of all diagnostic procedures
   g. A menu tree for each subsystem
   h. Setup procedures for each component of the subsystems
   i. A list of manufacturers, their local representatives, and subcontractors that have performed Work on the Project
   j. Installation and service manuals for each piece of equipment
   k. Maintenance schedules for all installed components

4. Operation and Maintenance Manuals shall include a separate section for each software program incorporated into the Project. The software section shall include, at a minimum, the following information:

   a. Definitions of all software related terms and functions
   b. Description of required sequences

c. Directory of all disk files
d. Description of all communications protocols, including data formats, command characters, and a sample of each type of data transfer
e. Instructions for manufacturer supplied report generation
f. Instructions for custom report generation
g. Database format and data entry requirements

E. Procedure for Resubmitting

1. Make corrections or changes in O&M's and/or Record Drawings as required by the Owner and resubmit to the Owner.

2. Clearly identify changes made other than those specifically requested by the Owner when resubmitting Record Drawings. Changes shall be clouded or similarly highlighted as coordinated with the Owner. Only changes that have been specifically requested by the Owner or have been clouded by the Contractor will be reviewed on resubmittals.

3. Any drawing sheets added to the resubmittal shall be clearly identified and clouded, and shall not change the sheet numbering scheme for previously issued Record Drawings.

4. The Contractor shall be responsible for any delays caused by the re-submittal process.

5. Re-submittal Review Fees

a. If the Owner rejects the Contractor's Record Submittal (Rejected, Revise, and Resubmit) more than two times, the Owner will be compensated for all subsequent reviews, whether partial or comprehensive. The amount of such compensation will be incorporated by Change Order and withheld from the Contractor's Application for Payment.

*****End of Section 28 05 00*****

SECTION 28 10 00 - ELECTRONIC ACCESS CONTROL AND INTRUSION DETECTION

1.01: Scope of Work

A. The Work shall include installation and commissioning of the following:

1. Integrated Security Management System (SMS) consisting of:
   a. Access Control and Alarm Monitoring System (ACAMS)
   b. Multi-Technology Access Control Readers
   c. Intrusion Detection Devices (IDS)
2. Interfaces
   ACAMS/CCTV
   ACAMS/Fire Alarm System
   ACAMS/VBS
   ACAMS/UPS
3. Miscellaneous:
   a. Wire and cable to install all equipment as specified herein.
   b. Conduit and back boxes (not shown on the Drawings as provided, but required for a complete installation).
   c. Equipment Racks and Enclosures required to house all equipment as specified herein.

B. Refer to Specification Section 28 05 00 Electronic Security Common Work.

1.02: Related Sections

1. Division 01 - General Requirements
2. Division 08 - Openings (Door Hardware)
3. Division 11 - Equipment
4. Division 26 - Electrical
5. Division 27 - Communications
6. 28 05 00 - Electronic Security Common Work
7. 28 23 00 - Electronic Video Surveillance

1.03: Additional Requirements

A. Refer to Specification Section 28 05 00 Electronic Security Common Work, for additional Part 1 - General requirements.

2.01: Access Control and Alarm Monitoring System Overview

A. The Contractor shall furnish and install a new Access Control and Alarm Monitoring System (ACAMS), access control equipment, system devices, and alarm monitoring equipment. The system provides local operational control of all access points and alarm sensors.

B. The ACAMS shall consist of a network controller, security workstations, software, and other required peripheral access control hardware and device. New equipment shall be provided as

required, such as Network Nodes (intelligent controllers IC's), card readers, and all other components as indicated on the Drawings and specified herein. Reference the Drawings for system configuration requirements.

C. The ACMAS shall incorporate distributed processing. ICs shall provide an intelligent interface between point monitoring and access control devices and the Network Controller. ICs shall collect point monitoring and access control messages from field devices, multiplex, and transmit the data to the file Network Controller and security workstations.

D. The ACAMS Network Controller shall be used in conjunction with Network Nodes (intelligent control panels IC's or data gathering panels DGP's) to provide a distributed access control and alarm monitoring system. In the event of a communications failure between the Network Controller and the IC, the IC's shall continue to make local access control decisions and save all transactions in memory until communications are restored. At that time the IC's shall upload all stored transactions to the Network Controller.

E. The ACAMS shall seamlessly integrate the functions of access control, alarms monitoring and response, digital video imaging and badge design/creation, and visitor management.

2.02: General

A. The security management system shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.

1. The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network-connected PC with a browser.

2. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

3. Security of the data communicated over the network to and from the browser, network controller, and nodes is protected by encryption (SSL 128-bit) and authentication (SHA-1).

4. The top hardware tier is the network controller. Embedded on the Network Controller are an operating system, a web server, security application software, and the database of personnel and system activity.

5. The middle hardware tier is the network node. The network node shall make and manage access control decisions with data provided by the network controller, and it shall manage the communication between the network controller and Application blades connected to the system's inputs, outputs, and readers. This modular design makes it possible, even during network downtime, for the system to continue to manage access control and store system activity logs. When network connectivity is re-established, the system activity logs are automatically re-integrated.

6. The bottom hardware tier is the Application Blades. Four unique Application blades shall be available:
   a. Access Control Blade: shall support two readers, four supervised inputs, and four relay outputs.
   b. Alarm Input Blade: shall support eight supervised inputs.
   c. Relay Output Blade: shall support eight relay outputs.
   d. Temperature Blade: shall support eight analog temperature sensor inputs.

B. The security management system shall integrate, within a browser interface, access control, alarm

monitoring, video monitoring, and temperature monitoring applications. These applications shall be embedded in three-tier software architecture.

1. The database tier shall use PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database that is embedded without requiring the use of a separate PC server.
2. The web server tier shall be based on an Apache™ embedded web server. This shall provide a graphically rich security management application through a standard web browser.
3. The web browser shall provide UL 1076 compliant browser-based monitoring and incorporate asynchronous Javascript™ and XML technology (AJAX) for a faster user experience.
4. The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.
5. This three tiered embedded software design runs within an embedded Linux operating system and shall require no client-side software other than a web browser.

C. All equipment and materials used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.

D. All security management systems and components shall have been thoroughly tested and proven in actual use.

E. All security management systems and components shall be provided with an explicit manufacturer warranty of one year for software and two years for hardware.

F. The ACAMS shall be an enterprise level security management system, capable of expansion to support no less than 3,584 card readers from a single Network Controller.

1. Network Controllers shall be available in various configurations, to support the following minimum card reader capacities: 64, 256, 896, or 3,584.

2.03: Acceptable Manufacturers of the ACAMS System shall include:

A. S2 Security Corporation

B. Approved equal

2.04: Overall System Capability

A. The security management system shall meet the requirements of business and government access control systems. The system shall monitor and control facility access, and shall perform alarm monitoring, camera and video monitoring, communications loss monitoring, and temperature monitoring. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions. The system shall be controlled from a web browser and require no software installation or client licenses. The system shall provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN), wireless networks, and the Internet. The system shall provide email and/or text message alerts for all alarm conditions and threats.

B. Widget Desktop: The security management system shall provide a widget-based user interface that

enables users to create custom monitoring layouts by selecting and arranging widgets on a desktop. Each widget shall provide easy access to a frequently used function—allowing users to, for example, view an activity log, a camera view, or real-time web content. System administrators can save custom layouts for subsequent call up by users, who can then arrange the widgets as desired on their desktops. The administrator shall determine which widgets are available in a layout and the extent to which users can customize the layout.

C. System Partitioning: The system administrator shall have the ability to divide the system database into partitions, allowing subsets of the overall population and/or resources to be managed separately.

1. From the default Master partition, one or more additional partitions can be created.
2. Each partition shall contain some number of administrators, card holders with their credentials, and resources.
3. When performing administrative functions, the administrator of a partition shall have the ability to affect only the cardholders and resources in that partition. However, resources can be shared across partitions through the mapping of access levels from one partition to another.
4. System partitioning shall have a precision feature that allows administrators in one or more partitions to view and perform edit functions on person records that belong to another partition.

D. The security management system shall provide the following Access Control capabilities:

1. Integrated photo ID creation capability with video verification.
2. User interface secured access under encrypted password control.
3. System-wide timed anti-passback function.
4. Regional anti-passback with mustering and roll call functions.
5. Region occupancy counting and control.
6. “First-in-unlock” rule enforcement.
7. Multiple access levels and cards per person.
8. Detailed time specifications.
9. Simultaneous support for multiple card data formats.
10. Elevator control.
11. Access privileges variable by threat level.
12. Scheduled portal unlock by time and threat level.
13. Card format decoder quickly discovers unknown card formats.
14. Card enrollment by reader or keyboard.
15. Compatibility with various input devices, including biometric readers.
16. Activation/expiration date/time by person with one minute resolution.
17. Access level disable for immediate lockdown.
18. Use of Threat Levels to alter security system behavior globally.
19. Multiple holiday schedules.
20. Timed unlock schedules.
21. Scheduled actions for arming inputs, activating outputs, and locking and unlocking

portals.

22. Card enrollment reader support.
23. Counted-use access control.
24. Dual-reader portal support.
25. Integration with supported alarm panels.
26. Optional storage and recall of ID photos and personal/emergency data.
27. Up to 60,000 person records.

E. The security management system shall provide the following Monitoring capabilities:

1. Common alarm panel integration for disarm on access, and arm on egress.
2. Integrated alarm monitoring and event management with alarm panels.
3. Support for the direct viewing of IP cameras.
4. Integrated real-time IP, DVR, and NVR systems with stored video replay for events.
5. Provides alarms on video loss, video motion detection, and video restore events.
6. Virtual inputs for video loss and building-occupancy-limits-exceeded.
7. Provides alarms on communication loss and temperature variation.
8. Support for the creation of custom sets of alarm event actions.
9. Provides the ability to record video and link to video for alarm events.
10. Available video control and playback through the user interface.
11. Provides the ability to assign threat levels to various alarms according to severity.
12. Provides the ability to select up to 20 levels of priority for event actions.
13. Support for electronic supervision of alarm inputs.
14. Support for the use of output relays for enabling circuits under alarm event control.
15. A monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications.
16. Support for the creation of unlimited customized monitoring layouts through the use of widgets.
17. Graphic floor plans with active icons of security system resources.
18. System user permissions to grant whole or partial access to system resources, commands, and personal data.
19. Secure access to the user interface under encrypted password control
20. Delivery of alerts via browsers, email, and text messages.

F. The security management system shall provide the following Video Management capabilities:

1. Real-time video monitoring displays, including unlimited cameras simultaneously.
2. Playback of event-related video.
3. Video switching and video widget pop-ups based on access activity or event activation.
4. Integrated alarm inputs from the video management system.
5. Digital playback of video events.

6. Linking of video and events based on triggers provided by the security management system or video system.
7. Support for multiple DVR and NVR systems.
8. Multiple pre-programmed supported cameras.
9. Recall of photo ID and real-time image for comparison.
10. Monitoring and control through a web browser interface.
11. System user permissions to grant whole or partial access to system cameras and video resources.

G. The security management system shall provide the following Security Database capabilities:

1. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data.
2. Partitions: It shall be possible to partition the system to create independent, virtual security management systems for multiple populations.
3. Support for the sharing of access levels and user privileges across partitions in a system.
4. Built-in Open Database Connectivity (ODBC) compliant database for personal data.
5. LDAP integration for single-user logon authentication.
6. Up to 60,000 person records.
7. Network-secure API for external application integration.
8. Extensive and easy to use custom report generator.
9. User-defined data fields in personnel records.
10. Record recall by vehicle tag, name, or card.
11. ODBC compliant Database.
12. An API for adding to, deleting from, and modifying the database.
13. Storage of system user passwords and permissions.
14. Storage and recall of ID photos and emergency personal information.
15. Pre-defined reports on system configuration, system activity history, and people.
16. English-based query language for instant custom reports.
17. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software (such as Crystal Reports) shall be necessary.
18. Periodic backup to on-board flash ROM and optional network attached storage (NAS), including FTP servers.
19. Periodic archive creation for historical custom reporting and improved on-board database performance.
20. Email and text messaging (SMS) alert notifications.

2.05: Hardware Requirements

A. The security management system shall employ a modular hardware concept that enables simple

system expansion and utilizes a three-tiered hardware hierarchy:

1. At the top tier is the network controller, which shall contain the database engine, web server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the security management system, set configurations, monitor activities, run reports, and manage alarms.
2. At the second tier is the Network Node, an intelligent device with native TCP/IP support, which shall make and manage access control decisions.
3. At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras, or temperature monitoring points.
4. The network device shall run on existing building TCP/IP networks and shall be configurable for access from separate subnets, through gateways and routers, and from the Internet. A MicroNode shall also be available that combines an Access Control blade and Network Node.

B. Network Controller:

1. The network controller shall contain the operating system, database engine, web server, application software, and configuration data.
2. The network controller shall consist of a blade-style, circuit card that also combines a network node on the card. The network controller portion of the card shall contain a processor, flash memory, and a network switch. The network controller shall be supplied with 12V DC at a minimum of 3 amps. Internal battery backup shall supply sufficient power to provide for an orderly shutdown of the system in case of loss of external power. External battery backup shall be used to provide uninterrupted operation in the event of external power loss. The Network Node portion shall contain a serial port for communication with the Application blades and a network interface port.
3. The network controller shall be available in three configurations to support small to medium (Solid-State controller), large (Extreme controller), and ultra-large (Enterprise/Ultra controller) systems.
4. The Extreme Network Controller shall be available in wall-mount or 2RU rack-mount enclosure. It shall contain a motherboard with an Intel® Atom™ processor and solid-state disk drive. An Ethernet connector shall be provided for network connection.
5. Extreme Network Controller shall have the following minimum capacities:
    a) Nodes/MicroNodes 64
    b) Access control portals 256
    c) Access cards 150,000
    d) Access levels 512 per partition
    e) Concurrent system users 10
    f) Alarm input points 2000
    g) Control point outputs 2000
    h) Temperature monitor points 500
    i) IP, DVR, and NVR cameras Limited only by license
    j) Online event history log up to 40 Million records
    k) Ethernet switch ports 1
    l) Time specifications 512 per partition
    m) Time spec groups 64 per partition
    n) Time specs per group 8 per partition
    o) Threat Levels 8 per partition
    p) Threat Level Groups 32 per partition
    q) Holidays 30 per partition
    r) Access levels per person 16

s) Cards per person 100
t) Report Groups 50
u) Camera Groups 50
v) Concurrent system users: 5 (when using the Monitoring Desktop or Camera Views); 10 (when performing administrative tasks)

6. Provide ACAMS Extreme Network Controller, where designated by Owner. Extreme Network Controller shall be 2RU rack mount type.

C. The Network Node (intelligent controller IC, or DGP) shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Controller and Application blades connected to the system's inputs, outputs, and readers. The Node shall be supplied with 12V DC at a minimum of 3 amps. The Node blade shall supply all Application blades in the node with power. The Network Node shall be available in three configurations: a combined network controller/network node blade; a standalone Network Node blade, and a MicroNode with included Access Control blade. Each Network Node shall support up to seven Application blades except for the MicroNodes. Communications between the node and network controller shall be encrypted and authenticated (SHA-1). Each network node shall have the following capabilities:

1.	Application blades	7
2.	Access control readers	14
3.	Access Levels	512
4.	Portals	14
5.	Portal Groups	64
6.	Readers	14
7.	Reader Groups	128
8.	Supervised Inputs	56
9.	Input Groups	64
10.	Relay Outputs	56
11.	Output Groups	64
12.	Temperature Monitor Inputs	56
13.	Elevators	14
14.	Floors	52
15.	Floor Groups	64
16.	Credential storage	20,000
17.	Activity Log records	27,000

D. The Application blades shall interface with the network controller through the Network Node. The Application blades shall be blade-style circuit cards. There shall be four types of Application blades:

1. Access Control blade: shall support 2 readers (input devices such as keypads, RFID devices or Biometric readers), 4 supervised inputs and 4 relay outputs.

2. Supervised Input blade: shall support 8 supervised inputs. Supervised input connectors are 2-pin. The system shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

3. Relay Output blade: shall support 8 relay outputs. Relay output connectors are 3-pin. Both normally-open circuit and normally-closed circuit output devices are supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

4. Temperature blade: shall support 8 analog temperature sensor inputs. Temperature range shall be 32° to 158° F (0° to 70° C). Temperature precision within that range shall be ±1.0° F (±0.5° C).The MicroNode shall combine a Network Node and an Application blade capability in one enclosure. The Access Control blade portion of the MicroNode shall support two readers, one temperature input, four supervised inputs and four relay outputs. A MicroNode shall utilize 12VDC power at 3 Amps or Power over Ethernet (PoE) at the 802.3AF standard and be capable of supplying direct power to 2 readers, 2 motion REXs, and 2 door strikes.

2.06: Hardware Packaging Requirements

A. The security management system shall have various hardware enclosures and configurations available to support different installation requirements. Enclosures shall be available for wall or rack mounting. The wall-mount enclosures shall have a lock requiring a key, and a cabinet door tamper switch.

B. The Wall-Mount enclosure supports one solid-state network controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 17" (432 mm) H x 15" (381 mm) W x 6.75" (171.5 mm) D.

C. The 4U Rack-Mount enclosure supports one solid-state network controller/Node blade or a standalone Network Node blade and seven Application blades. The dimensions are: 19" (483 mm) W x 7" (178 mm) H (4U) x 15" (381 mm) D.

D. Extreme network controller wall-mount units shall be housed in an enclosure with dimensions of: 12" (304.8 mm) W x 14" (355.6 mm) H x 3.5" (88.9 mm) D. The rack-mount unit dimensions shall be 2U rack x 12" (304.8 mm) D.

E. Enterprise network controllers shall be housed in a 1U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 1.75" (0.7 mm) H x 16.75" (425 mm) D.

F. Enterprise ultra network controllers shall be housed in a 2U rack-mount enclosure with dimensions of 19" (483 mm) W (including the mounting brackets) x 3.5" (1.4 mm) H x 16.75" (425 mm) D.

G. The MicroNode enclosure shall support a solid-state Node, its Access Control blade, and one temperature point.

1. It shall be a wall-mount enclosure with dimensions of 7" (178 mm) H x 7" (178 mm) W x 3.5" (89 mm) D.

2. It shall be possible to power the MicroNode with a 12VDC power source at no less than 2 Amps, or with PoE that conforms to the IEEE 802.3af standard. This provides nominal 48VDC at a maximum of 400mA.

H. The solid-state controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 3 amps. Power must come from a separate circuit with an isolated earth ground. If AC power is supplied it must be connected to the internal power supply. If DC power is supplied the internal power supply shall be bypassed. It shall be possible to backup power supplied to the security management system with an Uninterruptible Power Supply (UPS). It shall also be possible to

place within the wall-mount enclosure an SLA battery backup sufficient for an orderly shutdown in case of external power loss.

I. Enterprise controllers shall be powered by 100-240V AC at 50-60 Hz. Power must come from a separate circuit with an isolated earth ground and it must be connected to the internal power supply. It shall be possible to backup power supplied to the rack-mounted Enterprise and Enterprise Ultra controllers with an Uninterruptible Power Supply (UPS).

2.07: Network Controller, Node, and Application Blade Specifications

A. Application blades shall receive 12VDC power via the ribbon cable bus directly from the Node on the controller. The solid-state controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 3 amps.

B. Extreme Network Controller minimum specifications

1.	Network Nodes Supported:	64
2.	Processor:	Intel® Atom™ 1.6 GHz
3.	RAM:	1 GB
4.	Solid-State Disk Drive:	8 GB, 64 GB optional.
5.	Ethernet Ports:	1 (10/100)
6.	Operating Temperature:	32° to 95° F (0° to 35° C)
7.	Relative Humidity:	95% at 40° non-condensing
8.	Power Supply:	10 W, 85 to 260 VAC
9.	MTBF:	117,000 hrs
10.	Weight:	Rack-mount: 7.5 lbs. (3.4 kg)
11.	Heat Output:	82 BTU
12.	Storage:	8 GB SSD, optional 64 GB SSD
13.	Storage Temperature:	-20° C - 70° C
14.	Electrical Certification:	CE, FCC Part 15
15.	Environmental Certification:	RoHS, WEEE
16.	Capacity Rating:	10 eps

C. MicroNode: Each MicroNode shall function as a node and as an access control blade. In addition each MicroNode shall support one temperature input. The MicroNode may be supplied with 12VDC at 2 amps. With a 12VDC 2A power supply the total power available for all external output is 1100mA (13.2 watts). Alternatively, it shall also be possible to power the MicroNode by PoE that conforms to the IEEE 802.3af standard. This provides nominal 48 VDC at a maximum of 400mA. With PoE as the power source the total power available for all external 12V output is 500mA (6 watts).

1.	7-pin reader connectors	2	
2.	Maximum reader wire length		500 feet (152 m) (18 AWG twisted, shielded)
3.	2-pin supervised input connectors	4	
4.	Maximum input wire length		2000 feet (610 m) (22 AWG twisted,

shielded)

5. 3-pin relay output connectors 4
6. Maximum output wire length Determined by the peripheral device
7. 2-pin analog temperature inputs 1
8. Maximum temperature wire length 1000 feet (305 m) (18 AWG twisted, shielded)

D. Access Control blade: The access control blade shall receive power via the ribbon cable bus directly from the Node Blade. The access blade shall supply up to 400 milliamps of power to one reader or 200 milliamps of power to each of two readers.

1. 7-pin reader connectors 2
2. Maximum reader wire length 500 feet (152 m) (18 AWG twisted, shielded)
3. Power available to readers 400 milliamps
4. 2-pin supervised input connectors 4
5. Maximum input wire length 2000 feet (610 m) (22 AWG twisted, shielded)
6. 3-pin relay output connectors 4
7. Maximum output wire length Determined by the peripheral device

E. Input blade: The input blade shall receive power via the ribbon cable bus directly from the Node Blade. It shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

1. 2-pin supervised input connectors 8
2. Maximum input wire length 2000 feet (610 m) (22 AWG twisted, shielded)

F. Output blade: The output blade shall receive power via the ribbon cable bus directly from the Node Blade. Both normally-open circuit and normally-closed circuit output devices shall be supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

1. 3-pin relay output connectors 8
2. Maximum output wire length 2000 feet (610 m) (22 AWG twisted, shielded)

G. Temperature blade: The temperature blade shall receive power via the ribbon cable bus directly from the Node Blade.

1. 2-pin analog temperature inputs 8\
2. Maximum temperature wire length 1000 feet (305 m) (18 AWG twisted, shielded)

2.08: Software Requirements

A. Operating System and Application Software:

1. The embedded operating system for the solid-state network controller shall be Linux®.

The disk-based enterprise network controllers shall use Ubuntu 10.04 LTS (long term support) as the operating platform. The operating system kernel shall be open-source and no operating system training or certification shall be necessary.

2. The security management system application software shall be embedded in the system. The database shall be an embedded PostgreSQL relational database requiring a small footprint and provides high reliability. The web server shall be based on an embedded Apache™ web server enabling users to access and operate the system using a standard web browser.

B. Software Licensing:

1. Software licensing shall be based upon the number of readers and cameras for one network controller board. Software license upgrades shall be available if system reader and camera capacity must be raised. The user license shall be valid in perpetuity and shall include one year of software updates from the date of shipment from the factory.

2. Licensing shall be controlled by a Product Key and an Activation Key. The Product Key contains the licensed system features and limits. To upgrade your system license to enable more cameras or more doors you will need a new Product Key. The Activation Key contains the warranty expiration date. The keys are locked to the system license number. The system license number shall be viewable on-screen on the Support : About page

C. Software Upgrades: Software upgrades shall be possible from a browser on any network-connected PC, by uploading a software update to the controller. Controllers shall automatically upgrade all connected nodes. No client software installation shall be necessary.

D. Online Help and Documentation: The security management system shall be provided with complete embedded documentation. The on-line documentation shall include:

1. Context-sensitive online Help. (The Help displayed is specifically relevant to the current screen.) The online Help system shall provide explanations and procedures for all monitoring, administrative, and system configuration and maintenance functions. The Help system shall have linked table of contents, a linked index, and frequently asked questions pages. Each topic shall also have links to related topics. Each Help topic shall be printable.

2. Technical Support Notes: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

3. Installation Guides: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

4. Video Integration Guides: These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

5. System Administration Guide: This document shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics

6. The Help system shall also be available in a zip file format (xxx.zip) and it shall be possible to install the online Help system on any computer for purposes of reference and use by support personnel.

E. Support Collaboration: It shall be possible, by the use of a network Support Collaboration Tool, for a technical support specialist to connect to the security management system and assist on-site technicians from remote network-connected locations. It shall only be possible for an on-site system administrator or technician to initiate this connection. There shall be no way to initiate this connection from outside the secure network.

F. Language Support: The security management system shall be provided with multiple language support. The ability to switch from one language to another shall be accomplished through the user interface. Translation of the user interface, online help and documentation into other languages shall be available. The languages supported shall include:

1. English
2. Spanish
3. Portuguese
4. French
5. Italian
6. Thai
7. Chinese
8. Japanese

G. Date Formats: The security management system shall support global date formats as follows:

1. mm/dd/yyyy
2. dd/mm/yyyy
3. yyyy/mm/dd

H. Floor Plans: The security management system shall provide graphic floor plan capability including graphic display of links to other floor plans, alarms, system resources such as portals, IP video cameras, inputs, outputs, and temperature monitoring points.

1. The Network Administrator holding at least a 'Setup' user role shall be able to graphically configure device icons onto the floor plan images, and to upload additional floor plan images. JPEG images shall be supported, and the maximum size for a floor plan image shall be 256K.
2. It shall be possible to create floor plan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floor plan group is assigned to a particular system user then the floor plans in that group shall be viewable by that system user.

I. Personnel Data: The security management system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information.

1. All person data in the system shall be integrated onto one tabbed page for viewing, editing, and deletion by system users.
2. A system user holding at least an 'Administer' user role shall be able to create, delete, and modify person records, including access levels.

J. Data Import and Export: A Data Management Tool shall be provided that supports, via an API, the import and export of personnel data. This tool shall make possible the pre-populating, and ongoing populating, of cardholders into the security management system database. Data that shall be importable shall include:

1. LASTNAME
2. FIRSTNAME
3. MIDDLENAME
4. ACTDATE (activation date)

5. EXPDATE (expiration date)
6. NOTES
7. TEXT1...TEXT20 (user defined fields 1 through 20)
8. ACCESSLEVEL1...ACCESSLEVEL32
9. PERSONID
10. PIN
11. ENCODEDNUM1...ENCODEDNUM10
12. HOTSTAMPNUM1...HOTSTAMPNUM10
13. CARDFORMAT1...CARDFORMAT10
14. BADGELAYOUT
15. JPEG ID PHOTO
16. CONTACT PHONE
17. CONTACT EMAIL
18. CONTACT SMS EMAIL
19. CONTACT LOCATION
20. OTHER CONTACT NAME
21. OTHER CONTACT TELEPHONE
22. OTHER CONTACT TELEPHONE2
23. VEHICLE 1 COLOR
24. VEHICLE 1 MAKE
25. VEHICLE 1 MODEL
26. VEHICLE 1 STATE
27. VEHICLE 1 LICENSE#
28. VEHICLE 1 TAG#
29. VEHICLE 2 COLOR
30. VEHICLE 2 MAKE
31. VEHICLE 2 MODEL
32. VEHICLE 2 STATE
33. VEHICLE 2 LICENSE#
34. VEHICLE 2 TAG#

K. Data Security:

1. Communication between the network controller and the browser shall be secured using SSL. In addition, administrative access to the security management application and the personnel data shall be password protected and controlled by roles-based authorizations.
2. Communication between the network controller and the Network Nodes shall be encrypted and authentication/tamper detection shall be done using the SHA-1 algorithm.

3. Communication between the network controller and other systems (when using the API) shall be secured using SSL and authentication/tamper detection shall be done using the SHA-1 algorithm.

L. Data Backups: It shall be possible to configure regular automatic database backups.

1. It shall be possible to back up a solid-state network controller to an on-board compact flash.

2. It shall be possible to back up an enterprise network controller to a built-in hard drive.

3. It shall also be possible to save backups from any controller to separate network attached storage (NAS) and file transfer protocol (FTP) servers.

4. It shall also be possible to setup regular automatic creation of database archive files.

M. On-board Data Management: Each night the security management system shall truncate a sufficient number of the oldest records held on-board to reduce the database to its set limit, if required. This shall create the needed storage space for additional system activity records. Truncation will be performed on a First-in, First-out (FIFO) basis.

N. Partitions: It shall be possible to create multiple partitions for the management of multiple security systems or multiple populations.

1. It shall be possible to limit access to the data and resources of one partition to those with permissions for that partition.

2. It shall be possible for each partition to have its own population, resources, rules, events, video management, log data, reports and network resources.

3. It shall be possible to grant Monitor, Administer, and Setup privileges for multiple partitions to the same user. It shall also be possible to create custom user roles for each partition.

4. Each partition shall require at least one Node.

O. User Roles and Permissions: There shall be 4 pre-programmed levels of User Roles, and a total of 16 possible Custom User Roles that can be configured in the system, with different permissions for each user:

1. Master Partition Monitor: These users may use the functions in the Monitor menu only within the Master (default) partition. Monitor functions shall include viewing the activity log, cameras, and floor plans.

2. Master Partition Administer: These users may use the functions of both the Administration and Monitor menus only within the Master (default) partition. Administrative functions shall include adding and editing person information in the enrollment database, issuing and revoking cards, generating reports, and performing database backups.

3. Master Partition Setup: These users may use the functions of the Setup, Administration, and Monitor menus only within the Master (default) partition. Setup functions shall include defining access control, alarm event behavior, camera settings, floor plan images and configurations, holiday and time specifications. Setup functions shall also include: designation of network resources such as time and DNS servers, email and network storage settings; performance of system maintenance such as database backup and restore, software updates and file cleanups; designation of time zone, daily backup schedule and enrollment readers.

4. Full System Setup: These users may use the functions of all menus in all partitions.

5. Custom User Roles: In addition to the roles above the system shall also support the

creation of detailed user permissions regarding which cameras, floor plans, elevators, events, access levels, portals, reports, and personal data fields the system user may see, edit, delete, or control.

P. Alarm Panels: The security management system shall be capable of integrating with alarm panels, arming the panels, disarming the panels, and triggering events based upon alarm panel status.

Q. Alarm Events: The security management system shall be capable of managing alarm events.

1. It shall be possible to delay an input's change to the Alarm state by a specified number of seconds. The range of delay options shall be .5 seconds or 1-120 seconds.

2. It shall be possible to associate specific actions with each alarm event. These actions may include, but are not limited to:
   a. Lock and Unlock portals.
   b. Activate and Deactivate relay outputs.
   c. Arm and Disarm input groups.
   d. Pulse outputs or output groups.
   e. Arm and Disarm alarm panels.
   f. Send emails and SMS messages.
   g. Move cameras to preset positions.
   h. Switch to a video monitor.
   i. Record video.
   j. Momentarily unlock portals.
   k. Display ID photos.
   l. Change the system threat level.
   m. Make entries in the activity log.
   n. Play a digital sound file.
   o. Display alarms in different colors.
   p. Set a priority for an alarm (one of 20 levels, with 1 being the highest).
   q. Require a duty log entry.
   r. Clear alarm automatically or require an acknowledgement.

3. A system user holding at least a "Setup" user role shall be able to create, delete, and modify alarm system inputs, input groups, outputs, output groups, alarm panels, and events.

4. It shall be possible to trigger events based on system activity such as:
   a. Video motion detection.
   b. Camera failure and camera restore events.
   c. Valid or Invalid card reads.
   d. Portals held or forced open.
   e. Valid card reads with a specified access level.
   f. Inputs entering an alarm state.
   g. High and low temperature events.
   h. Alarm panel arming failures.
   i. Alarm panel zone faults.
   j. Tailgating and passback violations.
   k. Occupancy limit violations.
   l. Zone empty violations.
   m. Node power failure, communication failure, timeout, and tamper events.

R. Activity Monitoring

1. The security management system shall support a monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications.

2. The system shall support the creation of custom monitoring layouts for the display of

live video, system activity logs, alarm notifications, ID photos, floor plans, duty log entries, and portal status displays.

3. It shall also be possible to view cameras, activity logs, and floor plans on separate monitoring pages within the application.

S. Network-based Camera and Video Surveillance: The system shall provide live IP video surveillance capability. The number of supported cameras shall be limited only by license. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

1. Presets: The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.

2. Views: The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras). The application shall provide a drop down pick list for selecting current views or naming of new views.

T. Access Control:

1. The security management system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.

2. Time Specifications: The system shall be capable of storing up to 512 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and an end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.
   a. Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.
   b. Time specifications shall function appropriately per node for the time zone specified for that node

3. Card Formats: The system shall support the use of readers that use the Wiegand Reader Interface. The system shall default to the Wiegand 26 bit format unless a different bit length format is created in the system. The system shall support but not require the use of the card facility code. The system shall also support the use of the Magnetic Stripe ABA track 2 card data formats.
   a. It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 32 different card formats. The system shall support card formats up to 128 bits.
   b. It shall be possible to reverse the read order of the bits in the facility code and/or card ID portions of a card format.
   c. It shall be possible to view and change the default parity bit definitions for a card format.

4. Access Levels: The system shall be capable of storing up to 512 access levels in each partition. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or reader group, and a time specification. It shall be possible to also assign an elevator

floor group to an access level.

5. First-in Unlock Rule: The system shall support the use of a first in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs. The unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the First-in Unlock rule is satisfied and the unlock time spec is valid.

6. Holidays: The system shall be capable of storing up to 30 holidays per partition. Each holiday must be assigned a unique alphanumeric name of up to 64 characters. The definition of a holiday shall require a start date and an end date. Holidays shall have the ability to span several days using only one holiday slot. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated then the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

7. Portals: A portal is any access point and each portal supports up to two access reader devices. The System User, holding at least a "Setup" user role, shall be able to view current portal definitions, change portal definitions, delete portals, and create new portals. Creating a portal defines the access and alarm behavior of the access point. This can include:
   a. Card readers and keypads.
   b. Output for locking.
   c. Input for monitoring the door switch.
   d. Input for a Request-to-Exit function.
   e. Local alarm outputs and system alarm events.

8. Portal Groups: It shall be possible to create groups of portals and to assign an unlock time specification to the entire group. All the portals in the group shall remain unlocked during the time specified.
   a. It shall be possible to use portal groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a portal group is assigned to a particular system user then the portals in that group shall be viewable and unlockable by that system user.

9. Portal Alarm Conditions: Portals shall have four alarm conditions. The four alarm conditions are as follows:

10. Forced: When a portal is opened and there has been no card read, nor request to exit.
   a. Held: When a portal is held open past the expiration of the shunt timer.
   b. Invalid: When the portal reader reads a card for which there is no entry in the database.
   c. Valid: When the portal reader reads a card for which there is a valid entry in the database.

11. Two-man entry restriction: It shall be possible to require two valid card reads by different cardholders within a specified number of seconds for entry to a specific portal.

12. Anti-passback: The system shall support both regional and timed anti-passback access control. For anti-passback functions, it shall be possible to configure regions, assign readers to those regions, and specify events for response to tailgate, passback, and occupancy limit violations. It shall also be possible to designate parent regions for hierarchical anti-passback.
   a. Grace: It shall be possible for a system Monitor or Administrator to Grace card holders from passback and tailgate violations.
   b. It shall also be possible to set a specific time for all cardholders to be Graced daily.
   c. The system shall be able to automatically place the cardholder in a predefined

region upon the selection of the grace option

13. Mustering: To aid in evacuation management it shall be possible to designate a region or regions for mustering. It shall be possible to quickly get an occupancy count and occupant list for any region.

14. Scheduled Actions: It shall be possible to specify system actions to occur at scheduled times. These actions can include:
    a. Arming and disarming inputs.
    b. Activating and deactivating outputs.
    c. Locking and unlocking portals.

15. Floor plans: The system shall be capable of displaying active graphic floor plans and configuring each floor plan with icons representing system resources: cameras, portals, temperature points, and alarms. A network administrator holding at least a 'Setup' user role shall be able to upload floor plan images and graphically configure device icons onto the floor plan images. Viewing floor plans will require the Macromedia Flash Player 9.0 plug-in for the browser.
    a. It shall be possible to create floor plan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floor plan group is assigned to a particular system user then the floor plans in that group shall be viewable by that system user.

16. Elevator Control: The system shall be capable of controlling elevator access to floors. The system shall be capable of controlling up to 52 floor buttons per node. It shall be possible to create, change, or delete floor groups to assign a free access time specification to a floor group. The floors in this group will be freely accessible during the times defined by the chosen time specification.
    a. It shall be possible to create elevator groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If an elevator group is assigned to a particular system user then the elevators in that group shall be viewable by that system user.

17. An security management system user holding a "Setup" user role shall be able to create, delete, and edit access control specifications.

U. Threat Levels:

1. It shall be possible to configure up to eight threat levels. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be created and assigned to portal groups, access levels, input groups, output groups, floor groups, and event actions. The behavior of groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.

2. The security management system shall support 32 threat level groups.

3. It shall also be possible to change the system threat level in response to an alarm event.

4. The current system threat level shall display in the title bar of the security application interface and on floor plans.

V. Reports:

1. The security management system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy to use query language shall be included to create ad hoc reports. The query language shall be documented in the online help system. Alternatively, it shall be possible to specify a query by use of point-and-click.

2. It shall also be possible to produce reports directly from the network controller based on data in archive files on FTP servers, network attached storage, or the controller-attached compact flash.

3. The security management system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.

4. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

5. Report generation shall not affect the real-time operation of the system.

6. The specific reports provided shall include the following:
   a. Configuration Reports
   b. As Built: A graphical report that displays an image of each Application blade in a node and the specific resources (inputs, outputs, readers, etc.) configured for that blade. The network settings for the node shall also be included.
   c. Cameras: Displays all camera configuration information including control address, IP port, and camera type.
   d. Camera Presets: Displays configured presets for each camera in the system.
   e. Elevators: Displays elevator configuration information including Node, Reader, and Floor to output mappings.
   f. Floor Groups: Displays all configured floor groups for use in elevator control.
   g. Holidays: Displays holiday specification information.
   h. Portals: Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.
   i. Portal Groups: Displays a list of all defined portal groups.
   j. Reader Groups: Displays defined groups of readers.
   k. Resources: Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.
   l. Threat Level Groups: Displays all configured threat level groups and the threat levels assigned to them.
   m. Threat Levels: Displays all configured threat levels including the description and color assignment.

7. History Reports
   a. Access History: Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection.
   b. Custom Report: This provides the capability to create custom reports of historical data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.
   c. General Event History: Displays time, type of activity, and activity details for a variety of event types. The system user can select the specific event types for the report.
   d. Portal Access Count: Display how many times users have used a portal.
   e. Audit Trail: Displays an audit trail of system changes and the name of the system user that made the changes. It shall be possible to specify the dates and times covered in the report.

8. People Reports
   a. Access Levels: Displays all access levels entered into the system including time specification, reader/reader group, and floor group.
   b. Current Users: Displays a list of all security system users currently logged in to

the security system website.

c. Custom Report: This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet
d. Occupancy: Displays a list of defined regions with the number of people currently occupying each region and the maximum number of occupants allowed, if a maximum has been specified.
e. Photo ID Gallery: Displays all the photo ID pictures in the system and the person's name.
f. Photo ID Requests: Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.
g. Portal Access: Lists people with access for a selected portal.
h. Roll Call: Allows you to select a defined Region from the drop-down and see a list of people currently in that region.
i. Roster: Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.
j. Time Specifications: Displays all defined time specifications currently in the system.

W. Administration: The security management system shall provide for the performance of system administration tasks from any network-connected computer with a browser. Most of the administrative, maintenance, and configuration utilities and functions shall require a security management system user with at least a "Setup" user role. Information from the network administrator shall, in many cases, also be required. These administrative tasks shall include but not be limited to:

1. Database backups:
   a. The system shall create database, or full system data backups, each night at 00:15 hours. These backups shall be stored in ROM and compact flash onboard the solid-state network controller, and written to the drive on the disk-based controller.
   b. Backups shall also be written to network attached storage (NAS) or an FTP server if such storage has been configured in the system.
   c. It shall also be possible for the system users to create such database backups at any time. Any database backups onboard the network controller may also be downloaded to off board storage by the system user at any time.

2. System restore:
   a. The system shall be able to restore its database, or the full system data, from a backup. Restoration of the system shall only be possible from a backup copy onboard the network controller. It shall, therefore, be possible to upload a copy of a database backup from any network attached storage.
   b. It shall be possible to review backups by date and description and select the desired backup for upload to the network controller or restoration as the current system database.

3. Software updates:
   a. Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these .tgz files. Update of the application software shall only be possible from an update file onboard the network controller. It shall, therefore, be possible to upload a copy of the software update from any network attached storage or from any PC drive or desktop.
   b. Software updates may involve the network controller only or may include updates for the node(s) also. The monitoring of the security system may be

unavailable for several minutes during this process.

4. File cleanup: A utility shall be provided to assist in file cleanup. This utility will display for review and deletion all floor plan jpeg files, photo IDs, database backups, badge layouts, and software updates.

5. File upload: The system shall support uploads of files for use in and with the system. Files which shall be uploadable include:
   a. Floor plans in jpg format
   b. Badge layouts
   c. ID photos in jpg format
   d. Database backups
   e. Software license files
   f. software updates
   g. Threat level icons in jpg format
   h. Sound files (.wav) for use in event alerts

6. Setting system time, time zones, and time servers:
   a. The system shall support the setting of time zones by selection off of a drop down pick list. Time zones shall be separately settable for the controller and for each node or MicroNode in the system. An extensive list of world-wide time zones shall be provided. Adjustments for daylight saving time (summer time) shall be automatic.
   b. The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the network controller and its nodes will be regularly synchronized with the exact time used by all other network resources.
   c. It shall also be possible to manually set the system date and time.

7. Changing passwords:
   a. Person data maintained in the system may also contain a user name and password for logging on to the security application website as a system user. The system shall support the changing of administrator passwords. It shall be required to enter the password twice for verification purposes. Passwords may contain neither double-quote (“) nor single-quote (‘) characters.
   b. It shall also be possible to integrate a local law enforcement server for single-user logon authentication. This will reference the law enforcement-stored password for use by the system.

8. Issuing and revoking cards (credentials):
   a. Access cards shall be assignable by the system user either by entering card data directly into the person record or by use of an enrollment reader. Access levels shall be assignable through the user interface by selection from a drop-down list.
   b. Access cards shall be revocable at any time. A system user holding at least the Administer user role may perform this action. Revoked cards shall stop functioning immediately.

9. Enrolling new people: All person data entered into the system shall be held in the system database and shall be available only to system users holding at least the Administer user role. Person data can be added, deleted, and edited by such system users.

10. Generating reports:
    a. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.
    b. Alternatively, the system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt

for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.

c. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

d. A system user holding 'Administrator' permissions shall be able to view and create reports.

11. Configuring network resources:

a. LDAP: It shall be possible to configure an LDAP server for directory services and single-user login. This will reference the LDAP-stored password for use by the system.

b. DNS: The system shall support setting IP addresses for up to two domain name servers.

c. email settings: The system shall support the use of email notifications of alarm events. The system user must setup the email server IP address or DNS name and the email address of the network controller. A network administrator must setup the network mail server to relay email for the IP address of the network controller.

d. File transfer protocol (FTP): The system shall support the use of an FTP Server for backups. Once configured, backups are automatically saved to the FTP server each night.

e. NAS: The system shall support the use of network attached storage devices for backups. The network administrator must create a domain user account for the network controller and a password. The system user must configure the network attached storage in the system including the domain name, server IP address, share name, and the directory where the network controller may store data.

f. Time Servers: The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the network controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

g. A system user holding 'Setup' permissions shall be able to configure network resources.

2.09: Acams Security Workstations

A. Provide ACAMS security workstations as indicated on the Drawings.

B. All workstations shall run on a Microsoft Windows 7 or Windows 8 Enterprise Edition operating system platform.

C. All operator interfaces with the video surveillance system shall be through workstations. Workstations shall display real-time system messages, data files and records, operator instructions, data programming information, and custom graphic illustrations.

D. Workstations shall not be proprietary to the Contractor. The Owner shall be able to purchase additional workstations from computer vendors other than the Contractor.

E. Minimum System Workstation Specifications:

1. Dual core processor

2. Pentium IV or Xeon 2.8 GHz, minimum

3. 4 GB RAM

4. 40 GB Hard Drive

5. (2) Gbps Network Interface Cards (NIC)

6. 16X CD-RW and DVD-RW Drives
7. Two (2) USB Ports
8. 2 Com Ports
9. 32MB Video Memory
10. Mouse and Keyboard
11. Monitors:
    a. Provide (2) LCD monitors at each security workstation location, as indicated on the Drawings.
    b. 22" SVGA Monitor, minimum 1280x1024 Resolution
12. Operating System:
    a. Microsoft Windows 7 Enterprise Edition
    b. Microsoft Windows 8 Enterprise Edition
    c. Approved equal

F. All hardware and software shall meet the ACAMS manufacturer's minimum specifications for the supplied application.

G. Acceptable Manufacturers: Must meet Manufacturer's written recommendations.

2.010: Acams Peripheral Device Requirements

A. Equipment Power Supplies (for Network Nodes, IC's, and DGP's)

1. The Power Supply shall be dedicated to the intelligent panels, and shall not provide power for locks or any other low voltage device.
2. The Power Supply shall provide the following:
    a. 120 VAC 60 Hz input voltage and provide filtered and conditioned output voltage as required.
    b. Four (4) hours of battery backup to provide continuous operation during power failure.
    c. A battery charger to maintain the battery.
    d. Low battery and power fail contacts to monitor the status of the input power and the battery.
3. Each Power Supply shall be housed in a locking steel enclosure designed for surface mounting. The housing shall include a tamper switch to sense the removal or opening of the enclosure cover. All power supplies, IC's, DGPs, and power distribution cabinets shall be keyed alike.
4. Acceptable Manufacturers: As per the ACAMS manufacturer's recommendations and/or specifications.

B. Access Control Card Readers
    a. Card readers shall be consistent with Owner's selection for Hospitality Guest Room locking system.

C. Electrified Locking Mechanisms

1. General
    a. Electrified locking mechanisms shall be provided by the Door Hardware Supplier as required under Division-08 specifications, and where indicated on the Drawings.
    b. Interface with electrified locking mechanisms as indicated on the Drawings.
    c. Provide fail-safe operation of electrified locking mechanisms as required by

local codes.

d. Fail-secure locks shall remain operational during a fire alarm condition or power failure.

e. Refer to Division-08 Specifications and Door Hardware Schedule.

2. Electrified Locking Mechanism Power Supply

a. Provide power supplies for all electric locking mechanisms as specified with the exception of those noted as having time-delay functions as defined by NFPA 101.

b. Power supplies for time-delay function locks shall be provided by others. The Contractor shall coordinate with others as necessary to ensure proper operation of all time-delay electric locking mechanisms to include the provision of, and final termination of, system control and monitoring wire and cable as necessary to facilitate desired operation and integration with the system.

c. Provide power supplies for all electric locking mechanisms (with the exception of fire stair doors). Fail-safe locking devices shall unlock automatically under the following conditions:

1) Any building fire alarm
2) Loss of building power
3) Failure of the power supply

d. Provide battery chargers and batteries sufficient for four (4) hours of backup power for the connected load for all power supplies except those for fail-safe locks.

e. Monitor low battery and power fail alarms for each power supply.

f. Minimum Specifications:

1) Type: UL Listed Class II power limited
2) Input Voltage: 120VAC 60 Hz
3) Output Voltage: 24 VDC
4) Output Connections: Individually fused outputs to each lock
5) Output Rating: 150% of actual connected load
6) Battery: Sealed gel type
7) Alarm Outputs: Low battery and power fail
8) Enclosure: Steel enclosure with integral lock and tamper switch

g. Acceptable Manufacturers: Altronix, or Owner approved equal.

D. Door Position Switches

1. Provide concealed door position switches for each access controlled door indicated on the Drawings.

2. Normally closed (N/C) magnetic door position switches to monitor the open/closed status of doors as specified herein and as indicated on the Drawings.

3. Concealed Door Position Switch

a. Minimum Specifications:

1) Gap: ½" between the magnet and switch
2) Configuration: N/C
3) Mounting: 1" diameter hole in door and frame

4. Surface Mount Door Position Switch

a. Provide only where approved by Architect and Consultant.

b. Minimum Specifications:

1) Gap: 3" between the magnet and switch
2) Configuration: N/C
3) Mounting: Surface mount to door and frame

c. Provide armored cable from the switch location to the associated junction box in order to conceal the wire.

d. Acceptable Manufacturers: Refer to Division-08 Specifications and Door Hardware Schedule.

5. Overhead Door Position Switch
   a. Minimum Specifications:
      1) Gap: 3" between the magnet and switch
      2) Configuration: N/C
      3) Mounting: Floor
   b. Provide armored cable from the switch location to the associated junction box in order to conceal the wire.

6. Tamper Switch
   a. Provide normally closed tamper switches to monitor the secure status of all IC's, power supplies, and power distribution units.
   b. Include the number of tamper switches in the total alarm input figures.
   c. Minimum Specifications:
      1) Type: Plunger
      2) Configuration: N/C
      3) Mounting: Within cabinet with no outside access to fasteners

E. Request-to-Exit Devices

1. Request-to-Exit Devices may be integral to door exit hardware, may be PIR type, or may be push-button type.

2. Provide request to exit PIR device for each access controlled door indicated on the Drawings, unless request to exit device is integral to exit hardware, and provided under Division 08.

3. Passive Infrared (PIR) Device
   a. Request-to-exit (REX) infrared motion sensors for detecting authorized exits through card reader controlled doors as indicated on the Drawings. Wire the REX motion sensor to the REX input of the IC.
   b. For doors equipped with electromagnetic locks, activation of the REX motion sensor shall release the electric locking mechanism and shall shunt the intrusion alarm output.
   c. For doors equipped with electric locking mechanical that are free exiting at all times (i.e. mortise electric locks, electric strikes, etc.), the REX motion sensor shall only shunt the intrusion alarm output and shall not unlock the lock.
   d. Minimum Specifications:
      1) Detection tech: Passive Infrared
      2) Detection pattern: Adjustable narrow 15º cone
      3) Output contact: Two (2) Form "C" relay contacts
      4) Power requirements: 24V DC
      5) Mounting: Door frame lintel mounted or ceiling mounted
   e. Provide UL Class 2, power limited power supply as specified herein and/or as recommended by the device manufacturer.

F. Intrusion Alarm Devices

1. Detection devices shall be used for monitoring intrusion detection alarms.

2. Intrusion Detection Devices:
   a. Door Position Switches
      1) Door position switches shall monitor the open/closed status of doors for the purposes of intrusion detection.
      2) Door position switches utilized for these applications shall comply with requirements specified for card reader controlled doors defined herein.

b. Dual-Technology Motion Sensors
   1) Provide motion detection devices as indicated on the Drawings.
   2) Minimum Specifications:
      a) Detection technology: Passive Infrared and Microwave
      b) Detection pattern: minimum 35' range
      c) Output contact: N/C
      d) Listings: UL Listed
      e) Mounting: Surface, flush, or corner mount as per Drawings
   3) Provide the manufacturer recommended power supply. The power supply shall be UL Class 2, power limited.

G. Device Power Supplies

1. Provide Power Supplies for all ACAMS equipment.

2. Monitor low battery and power fail alarms for each power supply.

3. Minimum Specifications:
   a. Type: UL Listed Class II power limited
   b. Input: 120VAC 60 Hz hard wired
   c. Output: Regulated and filtered 24VDC
   d. Output rating: 150% of the actual connected load
   e. Battery backup: Four (4) hours of rechargeable backup
   f. Battery: Sealed gel type
   g. Alarm outputs: Low battery and power fail
   h. Enclosure: Key lockable wall mount housing with tamper switch

3.01: Requirements

A. Refer to Specification Section 28 05 00 Electronic Security Common Work, for Part 3 - Execution requirements.

*****End of Section 28 10 00*****

SECTION 28 10 00 - ELECTRONIC SAFETY AND SECURITY

D2810 SECURITY SYSTEMS

A. Applicable Codes and Guidelines:
   1. 2011 National Electrical Code with Local City of Bryan, TX Amendments
   2. ANSI/TIA/EIA-606-A – Administration Standard for Telecommunications Infrastructure of Commercial Buildings – Class 3
   3. All other local and state codes and standards shall be complied with where applicable and available

B. Access Control System:
   1. Design card access/access controls system for designated areas, minimally located as follows:
      a. Ingress locations throughout building
      b. Exterior Egress in Memory Care only
      c. Exterior Courtyard Gates
      d. Corridor Trespass from common area to back of house/service areas.
   2. Equipment shall include:
      a. Proximity type readers
      b. Software installed on dedicated PC, typically placed at main reception desk. Monitoring of cameras should be accessible to any computer connected to the network
      c. Access cards, FOBs, and RF Transmitters in quantity necessary

C. Surveillance System:
   1. Design for security cameras and motion sensors in designated areas, minimally located as follows:
      a. Independent Living Porte Cochère and Assisted Living Porte Cochère
      b. Exterior Service Entrance
      c. Licensed Care common corridors
   2. Equipment shall include:
      a. IP megapixel cameras and DVR
      b. Recording equipment located at locked/secure location such as MDF and/or IDF room
      c. Monitoring at main reception desk of all cameras
      d. Additional monitoring locations added via remote software

END

SECTION 28 23 00 - ELECTRONIC VIDEO SURVEILLANCE

1.01: Scope of Work

A. The Work shall include installation and commissioning of the following:

1. Integrated Security Management System (SMS) consisting of:
   a. Video Management System (VMS), or CCTV
   b. IP Based Digital Recording and Transmission System
   c. VMS Server and Client Workstations
   d. Network Switches (NS)
   e. Power-over-Ethernet (PoE) Devices
   f. IP-Cameras
2. Interfaces
   a. VMS/ACAMS
   b. VMS/NS
   c. VMS/UPS
3. Miscellaneous:
   a. Wire and cable to install all equipment as specified herein.
   b. Conduit and back boxes (not shown on the Drawings as provided, but required for a complete installation).
   c. Equipment Racks and Enclosures required to house all equipment as specified herein.

B. Refer to Specification Section 28 05 00 Electronic Security Common Work.

1.02: Related Sections

1. Division 01 - General Requirements
2. Division 26 - Electrical
3. Division 27 - Communications
4. 28 05 00 - Electronic Security Common Work
5. 28 10 00 - Electronic Access Control and Intrusion Detection

1.03: Additional Requirements

A. Refer to Specification Section 28 05 00 Electronic Security Common Work, for additional Part 1 - General requirements.

2.01: Video Management System

A. General

1. The Digital Recording and Transmission system shall offer the latest in digital technology, providing unparalleled stability, security, and ease of use, with advanced algorithms, fast capture rates, and a unique, flexible Graphical User Interface (GUI).
2. The system shall be a complete digital video monitoring and recording solution which may be a fully IP, server based application, or may utilize distributed network video recorders. The System shall provide for monitoring, controlling, and recording of all cameras in the System as indicated on the Drawings.

3. The entire System shall be color compatible, and all video shall be viewed and recorded in color. The combination of multiplexing, motion detection, audio, text insertion, image rates, mapping capabilities, and remote notification technologies shall provide an extremely flexible and reliable system.

4. The digital video compression technology shall utilize MPEG-4, H.264, or other approved AVC (advanced video coding) method.

5. Remote control of cameras with zoom lenses and pan/tilt drives through receiver/driver units. Receiver driver units shall be integrated into the camera dome enclosures. Remote control of the camera shall include pan, tilt, and zoom (PTZ), focus, and iris control. Remote control capabilities shall include automatic preset position control on alarm of PTZ cameras through the Security Workstation(s) via the Network Video Recorder(s).

6. Programming of automatic camera call-up of any camera on any monitor. Coordinate with the Owner to establish configuration guidelines and provide all initial programming.

7. Programming the alarm monitor(s) to be blank or display any video input signal when not in alarm condition. The CCTV shall automatically display alarm related video on the alarm monitor(s) when an alarm occurs. Following the specified dwell time, the CCTV shall return to the display selected before the alarm condition was initiated.

8. The Manufacturer shall provide access to Technical Online Support, Online Training using web conferencing, and 24/7 technical assistance and support via a toll-free telephone number at no extra charge.

9. The Digital Recording and Transmission System and its components shall be thoroughly tested before shipping from the manufacturer's facility.

10. The Digital Recording and Transmission System shall utilize the same user interface, regardless of platform, offering compatibility across the entire series.

11. The Digital Recording and Transmission system shall be accessible to authorized users via remote Internet Connection:
    a. Authorized users may include those such as local authorities having jurisdiction, and other entities as deemed necessary by the Owner.
    b. Once provided proper network configuration to allow access (through firewalls, etc), to the Owner's LAN, designated authorized users with Manufacturer's Remote Video Software shall be able to access the Digital Recording and Transmission system.
    c. Remote users which are authorized to access and view cameras on the Digital Recording and Transmission system would then be required to login with active User ID and Password, prior to accessing any camera video from the System.
    d. If allowable, Owner's Information Technology (IT) department would be responsible to provide necessary access through firewalls to local authorities requiring connection to the Owner's LAN for remote access to the Digital Recording and Transmission System.
    e. Contractor shall provide and install Remote Video Software application on up to five (5) Owner CPU's (either within or off-site from the facility), as designated by the Owner.
    f. Coordinate all work and requirements with the Owner and with other appropriate entities as necessary.

12. Video Surveillance System network connectivity requirements:
    a. IP Cameras, NVRs, and Client Workstations shall connect to the new Network Switches. New network switches shall be distributed as required through out the local IDF equipment rooms in the facility.

b. All Network Switches provided for the System shall be Power-Over-Ethernet (PoE) type, as required to power the IP Network PoE security cameras.
c. Contractor shall provide new PoE Network Switches, as required to fully support all requirements and components of the Video Surveillance System.
d. Distribute and size PoE Network Switches per equipment room, as required to support all IP security cameras as indicated on the Drawings.
e. Contractor shall coordinate all work and specific Network Switch types, quantities, and distribution locations with Owner prior to installation of components.

13. Digital video recording and storage configuration requirements:
a. The system shall be a complete digital video monitoring and recording solution which may be a fully IP, server based application, or may utilize distributed network video recorders.
b. Video may be stored locally on individual NVRs. NVR's shall be capable of automatically transferring recorded video to alternative, centralized video storage devices for longer term back-up storage.
c. Provide sufficient quantity and size of NVRs to accommodate all CCTV cameras indicated on the drawings, on a per equipment room basis.
d. Distribute and configure NVRs appropriately to provide the necessary digital video storage capacity for the System.
e. Each camera shall be capable of being streamed and recorded at 30 frames per second (fps) NTSC, at no less than 1280 X 720 HD 720p resolution, while maintaining bandwidth consumption during motion of no more than 3 MBps (megabits per second), with video stream set to variable bit rate.
f. Under normal conditions, each camera shall be streamed and recorded (recorded on motion only) at 15 frames per second (fps), at minimum1280 X 720 HD 720p resolution, while maintaining bandwidth consumption during motion of no more than 3 MBps (megabits per second), with video stream set to variable bit rate.
g. For storage calculation purposes, it shall be assumed that motion-based recording will occur 40% of the time for fixed cameras.
h. NVRs shall be sized, configured, and distributed throughout buildings and equipment rooms as needed to provide a minimum of 60 days of on-site video storage (on board the local NVR's/expanders) for each associated security camera.
i. Maintain 25% spare storage capacity on each individual NVR storage device when calculating minimum equipment requirements.
j. Maintain 50% spare video input channel capacity on each individual NVR when calculating minimum equipment requirements.
k. Provide additional NVR's as needed to accommodate all camera and video storage requirements.
l. Contractor shall, as part of the shop drawing submittal process, provide all video storage calculations, to thoroughly demonstrate that the quantity, size, and configuration of all NVR's meet the requirements of the specifications.

14. The Digital Recording and Transmission System shall be comprised of the following:
a. Video Management System Server
b. Video Management Client Workstations
c. IP Network Cameras
d. Network Switches
e. Digital Video Recorders and Storage Devices

2.02: Digital Video Recorder

A. The Digital Recorder shall include, as a minimum, the following features/functions/specifications:

1. The Digital Recorder shall be compatible with Local Area Networks (LAN) such as Ethernet, Token Ring, Cable Modems, DSL, FDDI, IP over ATM, IrDA (infrared), Wireless, and ATM-emulated LANs.
2. The Digital Recorder shall be optimized and designed for Microsoft Windows® Embedded XP, offering unparalleled stability, security, and ease of use, and shall allow the user to fully create and edit all network settings available with Windows Embedded XP.
3. The Digital Recorder shall come preconfigured with a DHCP enabled IP address and subnet mask to allow for installation in many IP settings without the need to reconfigure TCP/IP settings.
4. The Digital Recorder shall be available with eight (8), sixteen (16), or thirty-two (32) BNC composite video inputs. All models shall include corresponding BNC looping video outputs, with selectable termination via a dip-switch setting. The factory default setting of the dip-switches shall be termination on.
5. The eight (8) input Digital Recorder shall record at a rate of 240 images per second (ips), with real-time viewing of 30 ips per camera for live video.
6. The sixteen (16) input Digital Recorder shall offer recording options of 240 or 480 ips, with real-time live video viewing option available, each with 30 ips per camera
7. The thirty-two (32) input Digital Recorder shall offer recording options of 240 or 480 ips, with real-time live video viewing of up to sixteen (16) images, each with 30 ips per camera.
8. The Digital Recorder shall allow the user to adjust the resolution, quality, sensitivity, and number of images per second each camera will record. These adjustments shall be configurable per video input.
9. The Digital Recorder shall offer on board storage hard drive capacity from 4 Terabytes to 250 Terabytes.
10. The Digital Recorder shall be housed in a high-performance, metal case. The case shall be no higher than four (4) rack units (4U), and be designed to fit into a 19" EIA rack.
11. The Digital Recorder shall have 512 MB of system memory, and the processor shall be a minimum of an Intel® Celeron D. An internal 10/100 Network Interface Card (NIC) and a 128 MB video card shall be standard.
12. The Digital Recorder may include Hybrid (both IP network and analog video input channels) capabilities as a standard configuration.
13. The Digital Recorder shall include DDNS for free for the life of the Warranty. DDNS shall allow the operator to use a URL address instead of an IP address.
14. The Digital Recorder shall have the ability to easily backup important video to an internal or external media location, or an attached network storage device. The unit shall not stop recording during the backup process. To ensure the integrity of data, the digital recorder shall use a proprietary compression format that can only be read by the digital recorder's backup program; no other viewer can read the video.
15. The operator shall be able to monitor the status of the recording process by viewing a backup progress bar displayed on the main display screen. The backup progress bar shall automatically disappear from the main screen when the backup function has been completed successfully. The unit shall feature a "Scheduled Backup" option, allowing the operator to schedule the backup of video by date and time.
16. When backing up the video to a CD/DVD, the unit shall include the ability to record the video on to multiple CDs/DVDs, automatically prompting the user to insert the next CD/DVD when the previous CD/DVD is full.

17. The Digital Recorder shall include backup viewer software, allowing the user to playback the exported video in its proprietary format on a PC. The backup viewer shall have essentially the same search features as the digital recorder's software.

18. The operator shall be able to flag video clips distributed across multiple cameras. This feature will allow the operator to back up all clips from multiple cameras in one operation from the backup menu screen. The feature will allow the operator to add a memo to each video clip for review at a later date.

19. The Digital Recorder shall include a DVD-RW recorder allowing for up to 8+ Gigabytes of video data to be stored on each DVD and two (2) front accessible USB inputs as standard.

20. The Digital Recorder shall include a minimum of the following front panel controls, devices, and LEDs:
    a. Four Hard Drive Activity LEDs
    b. Power LED
    c. DVD-RW Drive
    d. DVD-RW Open Tray Button
    e. On/Off Power Switch
    f. Two USB inputs
    g. Fan Indicator LED
    h. One Hard Disk Drive Activity LEDs
    i. Four Hard Disk Drive Power LEDs

21. The Digital Recorder shall include a minimum of the following rear-panel connectors:
    a. 110V/220V auto-switching power-supply
    b. PS/2 Mouse Input
    c. PS/2 Keyboard Input
    d. USB Ports
    e. DB9 Serial Input
    f. LPT Parallel Printer Port
    g. Audio Line In
    h. Audio Microphone In
    i. S-Video Output (on Real Time models)
    j. SVGA Monitor Output
    k. RS-422/485 Interface (with RX, TX, and Operation LEDs)
    l. RCA Video Out
    m. RCA Audio Inputs
    n. RJ-45 Network Jack (with Activity and Link LEDs)
    o. Sensor/Alarm Inputs
    p. Control Outputs
    q. BNC Connectors for Analog Connections (if hybrid type)
    r. 75-Ohm termination dip-switches

22. All Digital Recorders shall include the following components from the manufacturer:
    a. PS/2 Mouse
    b. PS/2 Keyboard
    c. Digital Recorder (DVR) Repair Disc
    d. Remote Video Software Disc
    e. Power Adapter
    f. PTZ Adapter
    g. Rack mount attachments with screws
    h. Digital Recorder (DVR) key
    i. User Manual

23. The Digital Recorder shall come pre-configured for fast and seamless integration within existing IT infrastructures. The unit shall offer the following network setup options:

a. The ability to enable or disable access to the digital recorder from remote locations.
b. A designated time-out period that the connection will be terminated after unsuccessful user attempts to connect to the digital recorder.
c. An Emergency port used to connect with the Alarm Monitor Software.
d. A primary port used to connect to remote software.
e. An Image port used to transfer video to the remote software.
f. A Search port, used to transfer search information to the remote software.
g. The ability to enable or disable access by the Web Viewer Software, allowing a user to view live video using a Microsoft Internet Explorer browser.
h. The ability to adjust the resolution setting when sending video to remote clients.
i. The ability to throttle the bandwidth of the digital recorder to ensure that images and system messages are delivered as quickly as possible within the capabilities of the network's available bandwidth.
j. The ability to define the modem and PPP information to dial to a remote client when an Alarm Event is activated.
k. The ability to view the IP configuration of the digital recorder.

24. The Digital Recorder shall include an Alarm log to record and display information pertaining to alarm events, an Event log to record and display information pertaining to user logins, digital recorder reboots, configuration changes such as schedule and frame-rate changes, backup operations which will include user name, date & time, camera name and clip duration, and a System log to record/display hardware information pertaining to scan disks, system recording successes and failures, and other related information. The user shall have the ability to export the log information in one (1) week increments. These log files shall include the ability to be exported in their native format or as text documents.

25. The Digital Recorder shall include a User Management Console, which allows the user to create, edit, and delete user accounts. Each account can be assigned different privileges that limit the usage of the system. Privileges shall include, but not be limited to, the following functions:
a. Search
b. Setup
c. Pan/Tilt
d. Backup
e. Shutdown
f. Intensive
g. Forbidden Cameras
h. User Ranking
i. Auto Log Off

26. The Digital Recorder shall include Active Directory integration which allows domain user management tools to manage the digital recorder user accounts, Options shall include the ability to add and remove users from the digital recorder through group membership administration via a Windows domain controller, and a single sign-on feature that passes digital recorder user log on credentials to the video management and remote software.

27. To make managing a large amount of units easy and organized, the Digital Recorder shall allow the option of utilizing a Central User Management System. This option shall allow, from one location, the creation, deletion, and management of user accounts on multiple unit. The user accounts can be modified from any Digital Recorder as well as the Management Station. Any changes made on a unit shall be sent to the Management Station for broadcast to all units.

28. The Digital Recorder shall include a hidden camera feature, which allows an administrator to hide certain cameras from a user. The camera shall still be recorded, but the user will not be able to view the cameras in live or search mode.

29. The Digital Recorder shall allow the user to view the following system information:
    a. Video format of the digital recorder (NTSC or PAL).
    b. Software version of the digital recorder.
    c. The user specified unique identification name used by other software to connect to the digital recorder.
    d. The serial number of the digital recorder.
    e. A user specified contact number.
    f. Digital recorder manufacturer's technical support number.
    g. A note space for the user to type in any details about the system.

30. A Gigabit 10/100/1000 network interface adapter shall be available from the Manufacturer.

31. The eight (8) input digital recorder shall include eight (8) sensor inputs, for use with devices such as motion detectors, glass breakage alarms, door and window sensors, etc., and the inputs shall be configurable via software for Normally Open (NO), or Normally Closed (NC). The user shall have the option of setting a delay period of time (in seconds) before the alarm is activated, and shall have the option of displaying a sensor status bar on the main display screen, and when the operator places the mouse pointer directly over a sensor, the associated sensor title shall be displayed on the screen.

32. The sixteen (16) and thirty-two (32) input digital recorder shall include sixteen (16) sensor inputs, for use with devices such as motion detectors, glass breakage alarms, door and window sensors, etc., and the inputs shall be configurable via software for Normally Open (NO), or Normally Closed (NC). The operator shall have the option of displaying a sensor status bar on the main display screen, and when the operator places the mouse pointer directly over a sensor, the associated sensor title shall be displayed on the screen.

33. The digital recorder shall include the capability of recording either two (2), four (4), eight (8) or sixteen (16) of channels "Line-In" type audio (depending on model). The data size (per channel) shall be no more than 1,625 bytes per second.

34. During power-up, the digital recorder shall run a series of self-tests, and display messages as the various hardware and software sub-systems are activated. After power-up, the digital recorder's software shall load automatically and display the main screen.

35. The digital recorder's main video display screen shall include a minimum of the following buttons and features:
    a. Loop/Full Screen: Allows the operator to view the video display area using the entire viewing area of the monitor. The operator may also sequence through selectable screen division's sets, with an adjustable dwell time to specify the amount of time that elapsed before switching to the next screen division group.
    b. Second 16: On 32 channel units, displays the second set of sixteen (16) cameras.
    c. First 16: On 32 channel units, displays the first set of sixteen (16) cameras.
    d. Date/Time: Displays the current date and time. This date/time shall also be "stamped" into the recorded video and displayed whenever the video is played back.
    e. Search: Displays the search features that allow the operator to search previously recorded video.
    f. PTZ: Opens the options for controlling PTZ enabled cameras.
    g. Setup: Accesses the set-up menu from which all customizable settings can be edited.

h. Backup: Opens the backup options.
i. Login: Allows the login of a different user.
j. Exit: Allows Shut Down, Restart, Log On, Log Off and Restart in Windows Mode.
k. Current User: Displays the name of the user currently logged in to the digital recorder.
l. Remote Client Status: Displays whether anyone is connected remotely to the digital recorder.
m. Sensor Status Bar: Displays the sensor status for each camera that is set up to use sensors.
n. Control Output Status and Activation Bar: Displays the output status and allows the user to activate an output relay.
o. Screen Division Buttons: Allows the user to select the desired screen division to the video display area.

36. The camera status for each camera shall be displayed next to the camera number (or name) in the video display area. The information shall include:
a. Camera number and custom name.
b. Recording status, which shall show whether a camera is currently being recorded, whether a camera that has been set up for motion only recording is currently being recorded, or whether a camera is NOT currently being recorded.
c. Special recording status, which shall indicate whether a camera's associated sensor has been activated, and/or when the user activates the instant recording option for the selected camera.

37. Various screen division sets shall be available to the operator of the digital recorder.

38. The digital recorder shall allow for user definable, descriptive camera names of up to fourteen (14) alpha-numeric characters. The font size shall be adjustable, and the option to bold the characters shall be available.

39. To optimize the clarity and detail of recorded video, the digital recorder shall have the ability to adjust each video input's brightness, contrast, and hue. The user shall be able to easily return the video settings to the system's default, either individually or all at once, with a simple mouse click.

40. The digital recorder shall incorporate advanced video motion detection, including the ability to create multiple, complex detection regions, with adjustable sensitivity, per video input, utilizing "click and drag" of the system mouse. The operator shall have the option to select rectangle, circle or polygon region tools and layer non-motion regions over motion regions. Each region shall be resizable by dragging the sides and/or corners, and the operator shall have the ability to move each region anywhere within the setup area. The user shall be able to easily remove all motion regions from the setup area with a simple mouse click.

41. When motion occurs in programmed detection region, a colored box shall be displayed on the main screen around the region where the motion occurred.

42. The digital recorder shall include the option of displaying the associated video full screen upon a motion or sensor event, and enabling an audio alarm. The audio alarm shall be either a default beep, or a custom created sound file (.wav), unique to the application. The sound file shall be played through speakers attached to the digital recorder.

43. The digital recorder shall include the ability for pre-alarm and post-alarm recording, which shall record video for a specified time before and/or after a motion or sensor alarm has occurred. The time period shall be selectable from one (1) to sixty (60) seconds.

44. The digital recorder shall incorporate a "Regular Interval Recording" feature, allowing the unit to record a single frame every few seconds, every few minutes, every few hours, etc… to show that the unit is still functioning even when motion is not taking place. The amount of time shall be user programmable. This option shall only work when motion recording or sensor recording is selected.

45. The digital recorder shall include intensive recording, which allows the programmer to increase the pictures per second of any camera when a sensor or motion alarm event occurs.

46. The digital recorder shall include a video loss alarm function to allow an alarm event to occur when a camera loses signal for any reason (e.g. power failure, cable being cut, camera damage, etc…). When a video loss event occurs, the operator shall have the option to enable an alarm beep utilizing the internal speaker of the digital recorder, and/or activate an alarm output.

47. The digital recorder shall include a camera sabotage function to allow an alarm event to occur when the camera field of view experiences significant pixel change (e.g. changing the view of the camera, obscuring the lenses, significant shaking or vibration, or blinding light). When a video loss event occurs, the operator shall have the option to enable an alarm beep or a custom WAV file audible alert utilizing the internal speaker of the digital recorder, and/or activate an alarm output.

48. The digital recorder shall include Alarm Monitor software to stream video across a LAN to a client PC when an alarm is detected on the unit. The operator shall have the ability to stop, play forward and backward, frame by frame or real speed, the video that streams across. The program shall automatically load at startup and appear in the taskbar. It shall constantly monitor for a signal from the digital recorder, and when an alarm signal is detected The Alarm Monitor shall notify the operator of an event via a pop-up message window. An alarm beep shall also be activated to alert the user. The Alarm Monitor image viewer shall also allow the user to search through past events that have been recorded on the client PC.

49. To increase the amount of pertinent video that is saved by the digital recorder, and to keep it for a longer period of time, the operator shall have the ability to utilize recording schedules. For general installations, pre-defined schedules with basic configurations shall be standard. Up to thirty-two (32) user-definable recording schedules to maximize the recording efficiency of the digital recorder shall also be available. Schedules may be defined by the following:
    a. Day of Week.
    b. Time of Day
    c. Camera Number
    d. None, Continuous, Sensor Input, or Motion Recording
    e. Relay Output(s) Activation

50. Each of the digital recorder's thirty-two (32) detailed customized schedules shall allow the operator to "link" camera(s) and relay output(s) activation to particular sensor input(s). The schedules can be activated by date/time, motion alarms, and/or sensor inputs. Advanced options shall also be available that allows the user to send alarm events, either motion or sensor activated, to the remote emergency agent software or the video management software.

51. Instant recording shall be available to manually start a camera recording, superseding the current schedule. This recording shall be started by right-clicking the mouse and selecting Instant Recording on the desired video image, and the label "INSTANT" shall be placed on the upper right corner of the video. When this manual recording is activated, it shall automatically flag the specific video so that an index search can be performed at a later date for easy retrieval.

52. The digital recorder shall have the ability to export single images in the JPG file format, save video clips in the AVI format, or output to a VCR using the S-Video port. A digital signature shall be attached to every JPG and AVI file exported by the unit for use with the bundled Digital Verifier application. This function shall be unique to the unit and its verification software and shall not interfere with viewing files using other applications.

53. The digital recorder shall incorporate an internal RS-422/RS-485 adapter, with the ability to control multiple pan/tilt/zoom (PTZ) cameras. Depending on the model, control shall include multiple pan, tilt, zoom, and focus speeds, iris control (including return to auto-iris), focus control (including return to auto-focus), programming presets, and viewing presets. When an operator places the mouse pointer directly over a preset, the associated preset title shall be displayed on the screen.

54. The digital recorder shall support a large variety of protocols, to include those of most major CCTV manufacturers.

55. The digital recorder shall include on-screen play controls to playback the recorded video frame by frame (either forward or reverse), or play at normal speed (either forward or reverse). An on-screen hour/minute slide control bar shall also be available to allow the operator to select the hour and minute of the desired video. The slide bar shall be controlled either by clicking and dragging the slider, or using the wheel on the manufacturer supplied mouse.

56. The digital recorder software will include the ability to discover IP cameras of like manufacturer from the network with an integrated camera discovery protocol and add them to your digital recorder from a single interface.

57. The digital recorder software shall support a large variety of IP cameras, to include those of most major IP camera manufacturers.

58. The digital recorder shall support Megapixel IP cameras.

59. The digital recorder shall offer on-screen brightness controls to brighten up an image to get more detail, zoom controls to allow the user to digitally zoom in on an image, and speed controls to increase or decrease the playback speed. When recording images with extensive motion using 720x480 resolution, the unit shall offer the option of interweaving two frames to create a smooth detailed image, alleviating the “digital blur” that can interfere with the quality of the video when recording high speed moving images. This feature shall be activated with a simple mouse click.

60. The digital recorder shall include an option to enable Wide Screen support for monitors that output in 16:9 ratios. The feature shall allow the operator to switch between the standard 4:3 ratio and the widescreen 16:9 ratio.

61. The digital recorder shall include a time synchronization option, allowing a single channel of video to playback in real-time.

62. The digital recorder shall allow the operator to perform an index search based upon motion detection, sensor activation, instant record events, and/or ATM/POS transactions, greatly reducing the amount of time required to search through saved video. When searching ATM/POS events, the user shall have the option of searching for a specific transaction number, or searching for all transactions. A simple double-click on any one of the search results shall retrieve the associated segment of video.

63. The digital recorder shall include the ability to provide a twenty-four (24) hour visual overview of a single camera by separating a twenty-four (24) hour period into twenty-four (24) images, each representing the first second of each hour. The operator shall then have the ability to further narrow the search down to ten (10) minute and one (1) minute increments by simply double-clicking a displayed image.

64. The digital recorder shall allow the operator to specify a region on an image and perform a search based upon any motion that had occurred in that region. To indicate the progress of the search being performed, a status bar shall be displayed on the screen. The search results shall be displayed in a separate column, listed by date and time. A simple double-click on any one of the search results shall retrieve the associated segment of video.

65. The digital recorder shall include the ability to search for recorded video based of level of motion in the clip. A line graph that shows the level of motion in the clip will be displayed. The feature shall allow the operator to play back video where motion has reached the desired level of significance.

66. The digital recorder shall automatically adjust for Daylight Savings Time changes, with no loss of video when the hour jumps forward. When the hour falls back, the unit shall record both duplicated hours, and allow the operator to select which duplicated hour to play back.

67. The digital recorder shall allow the user to print a recorded image to a local or network printer, utilizing the printing options of the available printer.

68. The digital recorder shall allow for exporting single images in the JPEG file format, and saving video clips in an AVI format. This shall allow compatibility with any PC that supports these file formats. The AVI setup shall allow the user to enter a record duration and image quality setting as well as the desired codec from a pre-defined list.

69. JPEG images exported from the digital recorder shall be automatically digitally signed to verify the authenticity of the image, and ensure they have not been tampered with or edited in any way. A digital signature verification program shall be supplied with the digital recorder for installation on any computer. Using this program, the operator shall simply input the site code of the digital recorder that the image was originally extracted from, and press verify. If the image has not been tampered with, the program shall display the message “original image file”. If the image has been tampered with, the program shall draw a red square around the image and display the message “entire image changed” or “wrong site code”.

70. The digital recorder shall incorporate advanced hardware watchdog circuitry for unsurpassed system reliability.

71. The digital recorder shall include full integration of the Active Alert video analytics software allowing the operator to seamlessly configure and search Active Alert events within the primary server software.

72. The digital recorder software shall be provided with multi-language functionality.

B. The Video Management Software shall include, as a minimum, the following features, functions and specifications:

1. The video management software shall be a powerful utility that allows as many as one-hundred (100) Digital Recorders to be connected simultaneously and controlled using one (1) computer.

2. The video management software shall incorporate multiple screen divisions, allowing the operator to create several groups of cameras and customize the organization of the cameras. Each screen shall contain up to thirty-six (36) different cameras.

3. The video management software shall include the ability to have multiple windows open at any given time. The organization of these windows shall be done using tabs, and the operator shall have the ability to jump from one window to another by simply clicking on a given tab. The video management software shall also support the use of multiple monitors, allowing the user to view multiple windows simultaneously.

4. The video management software shall allow remote audio in both live and retrieval modes.

5. To allow users to quickly identify alarm zones and view the associated video, the video management software shall be capable of importing maps or linking to HTML maps and associating cameras and sensors to locations on the maps. The software shall allow for importing an unlimited number of maps.

6. The video management software shall allow the user to view different types of alarms that are coming from the unit, including video signal loss and sensor alarms. The software shall incorporate a filter button to filter through the different types of alarms. By simply double-clicking an alarm entry, the search window shall open with the associated unit, camera, and time related to the selected event.

7. The video management software shall log all alarm events with the available associated video. Up to fifty of the most recent events shall be viewable as on-screen thumbnail images. The operator shall have the ability to set the number of thumbnails and the display size. Up to nine display sizes shall be available.

8. The video management software shall include a health information window to view the health of units connected to the software. The window shall provide all the collected information related to the health of a unit at a given point in time. This information can be used to track data usage or monitor the stability of a unit over time to determine if components are in need of replacing before a critical failure.

9. The following shall be available in the health information window:
   a. Total Status: Indicates if the unit is healthy and running correctly.
   b. Network Status: Indicates if the network component of the unit is running correctly and error free.
   c. Disk Status: Indicates if the hard drives of the unit are running correctly and have available storage space.
   d. Video Status: Indicates if the video component of the unit is running correctly and error free.
   e. Recording Status: Indicates if the recording component of the unit is running correctly and error free.
   f. Digital Recorder: Displays pertinent information on the unit.
   g. Video/Recording:Displays the recording status of cameras connected to the unit.
   h. Memo: Space to input notes on the health check event.
   i. Disk Usage: Indicates disk usage and remaining available space.
   j. Export: Exports the unit's health information as an HTML document.

10. Upon a warning or failure of any of health attributes on the unit, the video management software shall display an icon indicating the type of error that occurred. The unit shall also include the option of sounding a voice warning if a failure is detected.

11. The video management software shall allow the operator to right-click any live camera and instantly capture a still JPEG image of the current camera field of view.

12. The video management software's network backup feature shall allow the operator to select the video to be saved and the location of where to save it. The software shall include a status bar to indicate the progress of the backup.

13. The video management software shall have several options to allow the operator to search through and find a particular section of video. The options shall include preview search, a search option that allows the user to narrow down recorded video in a 24-hour period, displaying one image for each hour of the day. When the image is selected, the hour chosen shall then be broken down into six (6) images, one image for every ten (10) minute increment. When an image is again selected, ten (10) images are displayed, one for every minute within the ten (10) minute period. The selected image can then be applied to the main search.

14. The video management software shall allow the operator to export single images in the JPEG file format and save video clips in the AVI file format. This shall allow compatibility with any PC that supports these file formats.

15. The video management software shall incorporate a log to keep track of when the software was opened and closed, and who logged in and out, The software shall also utilize an alarm log to allow the user to view different types of alarms coming into the system. Double clicking an entry shall open a search window with the associated digital recorder, camera, and time related to the event.

C. The Remote Video Software shall include, as a minimum, the following features, functions, and specifications:

1. The remote viewing software shall allow a user to fully operate and maintain the Digital Recorder remotely, and shall connect using standard TCP/IP protocol through connection types such as DSL, Cable Modems, T1, ISDN, or LAN connections.

2. The remote software shall provide the user with most of the features and functions available at the local Digital Recorder. The remote features and functions shall include viewing live video, searching through archived video, exporting images and video clips, and virtually all setup functions.

3. The remote video software shall allow up to five (5) users to simultaneously connect to a single Digital Recorder. Each user can perform functions on the unit and not affect the other users. The unit shall only allow one user to access the setup and PTZ functions at any given time.

4. To ensure that only authorized personnel are allowed to log in to the Digital Recorder, the remote video software shall utilize user accounts with assigned privileges, allowing or denying access to different functions.

5. Remote Video Software may be installed on additional client workstations or Owner provided CPU's, where designated. Manufacturer specifications recommend the following minimum CPU requirements:
   a. Pentium IV, 2.0 GHz or Equivalent
   b. 256MB System Memory
   c. DirectX 9 or Higher
   d. Compatible Video Card
   e. Internet or LAN Connection
   f. TCP/IP Installed
   g. Microsoft Windows 7 Operating Systems
   h. 1024 x 768 Display Resolution
   i. 32 Bit Color Depth or Better

6. Provision for Remote Video Software Application
   a. Contractor shall provide and install Remote Video Software application on up to five (5) Owner CPU's (either within or off-site from the facility), as designated by the Owner.

D. Physical specifications

1. Unit Dimensions (H x W x D): 7.0" x 17.3" x 21.75"

2. Unit Weight: 64 lbs.

3. Power Requirement: 100-240 VAC (50/60Hz), 10/7A

4. Operating Temperature: 40° - 104° F (5° - 40° C) non-condensing

E. Locate and rack mount devices in equipment racks in Telecom / Server rooms. Coordinate final locations with Telecommunications Contractor and with Owner.

2.03: Video Management System Server

A. Provide Video Management Server as indicated on the Drawings, to manage digital video recording equipment and IP network cameras.

B. The file server shall provide the following features:

1. Centralized control and management of the entire video surveillance system.
2. Communications with client workstations, NVRs, and IP cameras.
3. Centralized means of software update downloads/uploads.

C. Minimum Video Management System Server Specifications:

1. Dual core processor
2. 4 GB RAM
3. Dual Network Interface Card (NIC) or compatible pair of NICs, 1 Gbps.
4. 16X CD-RW and DVD-RW Drives
5. 3.5” 1.44 MB floppy disk drive
6. 1 TB backup drive
7. NovaBACKUP Two (2) USB Ports
8. 2 Com Ports
9. 32MB Video Memory
10. Graphics adapter which supports 32-bit color or higher
11. (1) 19” SVGA Monitor, minimum 1280x1024 Resolution
12. Mouse and Keyboard
13. Windows Media Player

D. All hardware and software shall meet the CCTV manufacturer’s minimum specifications for the supplied CCTV applications.

E. Acceptable Manufacturers: Dell, or Owner approved equal. Must meet Manufacturer’s written recommendations.

F. Locate and rack mount in local MDF, IDF, or security equipment room. Coordinate final location with Owner.

G. Contractor shall coordinate with Owner’s IT technical staff to assure that the Warranty and Maintenance for the Server is in registered in the name of the Owner.

2.04: Video Surveillance Client Workstations

A. Provide security workstations as indicated on the Drawings.

B. Provide (1) security workstation at the Manager’s office or as otherwise directed by Owner.

C. All workstations shall run on a Windows 7 Enterprise Edition operating system platform.

D. All operator interfaces with the video surveillance system shall be through workstations. Workstations shall display real-time system messages, data files and records, operator instructions, data programming information, and custom graphic illustrations.

E. Workstations shall not be proprietary to the Contractor. The Owner shall be able to purchase additional workstations from computer vendors other than the Contractor.

F. Minimum System Workstation Specifications:

1. Dual core processor
2. Pentium IV or Xeon 2.8 GHz, minimum
3. 4 GB RAM
4. 40 GB Hard Drive
5. (2) Gbps Network Interface Cards (NIC)
6. 16X CD-RW and DVD-RW Drives
7. Two (2) USB Ports
8. 2 Com Ports
9. 32MB Video Memory
10. Mouse and Keyboard
11. Monitors:
    a. Provide (2) LCD monitors at each client workstation location, as indicated on the Drawings. Provide dual channel video card to support dual monitors.
    b. 22" SVGA Monitor, minimum 1280x1024 Resolution
12. Operating System:
    a. Microsoft Windows 7 Enterprise Edition
    b. Owner approved equal

G. All hardware and software shall meet the CCTV manufacturer's minimum specifications for the supplied.

H. Contractor shall coordinate with Owner's IT technical staff to assure that the Warranty and Maintenance for the Client Workstations are registered in the name of the Owner.

2.05: CCTV Monitors

A. Provide monitor for all security workstations, where indicated on the Drawings.

B. All monitors shall operate at 120VAC 60 Hz.

C. 22-inch Color LCD Monitor

1. Minimum Specifications:
    a. Screen size/type: 22-inch TFT LCD
    b. Sync Format: NTSC/PAL
    c. Resolution: SVGA, 1280 x 1024
    d. TV Lines: 500 typical
    e. Aspect Ratio: 5:4
    f. Colors: 16.7 million
    g. Back Light: 4 cold cathode fluorescent tubes
    h. Contrast Ratio: 1000:1

i. Viewing Angle: 178 degrees, horizontal and vertical
j. Inputs: DVI, VGA, BNC, RGB, Composite Video, S-Video
k. Weight: approx 17 lbs.

2. Acceptable Manufacturers: As per CCTV System manufacturer's recommendations.

2.06: CCTV Cameras

A. Fixed IP Network Security Camera

1. Provide fixed IP network mini-dome security camera as indicated on the Drawings.

2. The camera shall be manufactured with a tamper-resistant casing and metal encapsulated electronics.

3. The camera shall be equipped with a progressive scan megapixel sensor, varifocal DC-iris lens with remote zoom and focus capabilities, Wide Dynamic Range, so called Day/Night functionality and shall provide images down to 0.4 lux in day mode and 0.06 lux in night mode.

4. The camera shall be equipped with a 10BASE-T/100BASE-TX Ethernet-port, and shall include support for Power over Ethernet according to IEEE 802.3af.

5. The camera shall provide simultaneous Motion JPEG and H.264 video streams and shall support at least two individually configured video streams of HDTV 720p (1280x720) resolutions in full frame rate (30 fps) using H.264. The H.264 implementation shall include both unicast and multicast functionality and support Constant Bit Rate (CBR) as well as Variable Bit Rate (VBR).

6. The camera shall be fitted with a built-in microphone, Line In and Line Out, provide full duplex audio, and shall support AAC, G.711 or G.726 compression.

7. The camera shall be equipped with one digital (alarm) input and one digital output, and shall also be able to trigger its embedded event functionality based on camera tampering alarm, detection of video motion or audio, or when the local storage is full. Possible response to a trigged event shall include remote notification, incl. video upload, and activation of output and recording to local storage. The camera shall be equipped with at least 48MB of memory and hold a SD/SDHC card slot for expanding the memory.

8. The camera shall feature overlay text ability, that includes date and time synchronized using an NTP server. Furthermore, it shall have the ability to apply a graphical image as an overlay and a privacy mask in the video stream.

9. The camera shall support both static IP addresses and addresses from a DHCP-server, and shall support both IPv4 and IPv6. The camera shall incorporate support for Quality of Service (QoS).

10. For secure access to the camera as well as provided content, the camera shall support HTTPS, SSL/TLS and IEEE802.1X authentication. The camera shall also support IP address filtering and include at least three different levels of password security.

11. The camera shall contain a built-in web server making video and configuration available in a standard browser environment using HTTP and shall also be fully supported by an open and published API (Application Programmers Interface) providing necessary information for integration of functionality into third party applications.

12. Indoor mini-dome cameras shall be recessed in to flush mount 4" square back-box.

13. Coordinate all back-box requirements, rough-in, and network connectivity requirements with the electrical contractor and telecommunications contractor.

14. Minimum Specifications
    a. Unit Dimensions (WxH): 4.9" x 4.9"
    b. Be manufactured with a tamper-resistant casing and metal encapsulated electronics.
    c. Be equipped with a 10BASE-T/100BASE-TX Ethernet interface
    d. Be equipped with a progressive scan megapixel sensor, support WDR and shall provide images down to 0.4 lux in day mode and 0.06 lux in night mode
    e. Be equipped with so called Day/Night functionality and a varifocal DC-iris lens supporting remote zoom and focus
    f. Provide at least two video streams at full frame rate (30 fps) in HDTV 720p (1280x720) resolution using H.264
    g. Support simultaneous individually configured Motion JPEG and H.264 video streams
    h. Support both unicast and multicast H.264 with support for both Constant and Variable Bit Rate
    i. Support Power over Ethernet according to IEEE 802.3af
    j. Provide 1 channel of full duplex audio and be equipped with a built-in microphone, Line/Mic In and Line Out
    k. Accept static IP addresses as well as addresses provided by a DHCP
    l. Support both IPv4 and IPv6 based addresses
    m. Provide text overlay that includes date/time support synchronized with an NTP server and the ability to apply a graphical image as an overlay into the video image
    n. Provide multiple user password levels, support for HTTPS and SSL/TLS and incorporate IEEE 802.1X authentication
    o. Be equipped with one digital (alarm) input and one digital output
    p. Include embedded event functionality, which may be triggered by:
        1) alarm input
        2) camera tampering alarm
        3) video motion detection
        4) audio detection
        5) local storage full
    q. Event actions supported by the camera shall include:
        1) remote notification, including video upload
        2) activation of output
        3) recording to local storage
    r. Be equipped with a built-in web server
    s. Be supported by an open and published API

15. Acceptable Manufacturers
    a. Axis P3344
    b. Approved equal

B. Integrated Pan/Tilt and Zoom (PTZ) IP Dome CCTV Camera

1. Provide PTZ IP dome cameras where indicated on the Drawings.

2. All PTZ IP dome cameras shall be 4CIF (704x480 pixels) minimum resolution.

3. The PTZ dome camera shall incorporate a day/night CCD camera, a minimum of 36X (use 18x max for garage PTZ's) optical zoom lens, an integral receiver/driver unit, and an integral pan/tilt drive.

4. The day/night camera shall be capable of sampling lighting conditions to automatically detect the necessity of switching between color and black and white modes.

5. The dome enclosure shall be tamper resistant, and sealed to protect from environmental conditions.

6. Cameras with PTZ capabilities shall be configured such that all alarm points or card reader controlled doors located within the available field of view are programmed as presets for automatic viewing and real time recording. Applicable alarms generated by the ACAMS shall cause the camera to pan around, tilt up or down as required, and zoom in on the alarm event. Verify all preset positioning with the Owner prior to programming.
   a. The Contractor shall provide a minimum of one (1) CCTV camera preset per viewable ACAMS point (i.e. alarm, activation, card reader, etc.), to the CCTV system for automated camera call-up.

7. Provide "environmental" outdoor version of PTZ dome cameras at all exterior locations shown on the Drawings. Environmental outdoor PTZ dome camera shall be equipped with integral heater/blower to accommodate for environmental changes.

8. PTZ Camera Minimum Specifications:
   a. Image device: 1/3" or 1/4" CCD, color
   b. Resolution: 4CIF minimum
   c. Signal to noise ratio: >50 dB
   d. Day/Night Mode: Yes, Automatic
   e. Sensitivity: Day (usable picture 50 IRE) 1.4 lux; Night (usable picture 50 IRE) 0.33 lux
   f. Synchronization: Internal or line lock
   g. Iris Control: Automatic
   h. Lens: 36x Zoom (3.4-122mm) (use 18x max for garage PTZ's)
   i. Digital Zoon: 12x
   j. Video Output: 1.0Vp-p, 75Ohm
   k. Pan speed: 0.1º to 150º/second, 250º/second for presets
   l. Tilt speed: 0.1º to 40º/second, 200º/second for presets
   m. Vertical Tilt range: +2º to -92º with "auto-flip" functionality
   n. Preset positions: 40 presets/dome with no more than +0.25º variation
   o. Video connection: RJ45 Ethernet (or provide IP module as necessary)
   p. Power requirements: 24VAC, 12VDC, or PoE
   q. Unit Weight: approx 7 lbs

9. Acceptable Manufacturers:
   a. Axis IP PTZ camera
   b. Approved equal

C. CCTV Camera Enclosure Mounts

1. Provide CCTV camera enclosure mounts as appropriate for the application and as specified herein.

2. Verify final location and mount type of all cameras with Owner.

3. The Camera enclosure mounts shall be provided for wall, pendant, corner, pole, and parapet mount applications.

4. The mounts shall be compatible and similar in design as specified camera enclosures.

5. The wall mount length shall not extend more than ten (10) inches from the wall to the enclosure base.

6. The pendant mount length shall not extend more than eight (8) inches from the ceiling to the enclosure base.

7. Each Camera Enclosure Mount shall be designed to adequately support each associated camera enclosure, which shall also include the weight of the camera, lens assembly, cable, and cable fittings.

8. The Camera Enclosure Mount shall employ an adjustable swivel/tilt head to allow for enclosure rotation as necessary to obtain the correct camera field of view. Unless otherwise noted, all cabling between the conduit junction box and camera enclosure shall feed directly though the enclosure mounts. All accessible cabling shall be armored for protection. At no time shall the cabling bypass the Camera Enclosure Mount and feed directly into the camera enclosure.

9. Provide all support structure as necessary to insure the Camera Enclosure Mount is securely fastened to the building structure.

10. Each camera mounting height and location shall be approved by the Owner prior to rough-in or installation.

11. Acceptable Manufacturers: As per CCTV System manufacturer's recommendations.

D. Camera Locations and Mounting Heights

1. Security Contractor shall coordinate all conduit and back-box requirements and locations with the Electrical Contractor, prior to rough-in.

2. Interior Cameras:
   a. Shall be ceiling mounted, as indicated on the Drawings, where ever possible.
   b. Wall mounted interior cameras, where required, shall be installed at 9' AFF, or 6" BFC, which ever is lower.
   c. Verify exact location of all cameras with Owner prior to rough-in.
   d. Coordinate all wire path way routing with Owner.
   e. Mini-dome ceiling mounted cameras shall be recessed in to flush mount 4" square back-box. Else provide recessed mounting kit. Mini-dome ceiling cameras shall not be surface mounted.
   f. Coordinate all back-box rough-in and network connectivity requirements with the electrical contractor and telecommunications contractor.

3. Exterior Cameras:
   a. Shall be wall mounted where possible, and shall be installed at 10' to 15' AFG.
   b. Provide wall mount arm or roof parapet mount where necessary.
   c. Cable path way to penetrate exterior wall into accessible ceiling space where possible.
   d. Verify exact location of all cameras with Owner prior to rough-in.
   e. Coordinate all wire path way routing with Owner.
   f. Coordinate all back-box rough-in and network connectivity requirements with the electrical contractor and telecommunications contractor.

2.07: CCTV Camera Power Supplies

A. Generally, CCTV power supplies should not be required for indoor cameras.

B. Indoor IP network cameras shall be PoE, and shall receive power from the PoE Network Switches or from PoE mid-span power injectors, provided by the Contractor.

C. If for any reason auxiliary power supplies are required to complete the System, Contractor shall provide all equipment and cabling as necessary.

D. Power-over-Ethernet (PoE) mid-span power injectors shall be provided if necessary.

1. Shall provide PoE to IP network security cameras.

2. Install Security PoE injectors in IDF rooms where needed. Coordinate mounting location in Telecom racks with Owner.

3. Minimum specifications

a. Unit shall be rack mountable, 1U height.
b. PoE ports: 8
c. Power output: 15.4W max per port
d. Shall be IEEE 802.3af compliant
e. Port status LED indicators
f. Automatic detection and protection for non-PoE cameras
g. Shall be compatible with supplied IP PoE cameras
h. Input power: ~115VAC
i. Shall be backed up by local security UPS device
j. Acceptable Manufacturers:
    1) Axis Power over Ethernet Midspan
    2) Altronix NetWay8
    3) Approved equal

E. PTZ Camera Power Supply

1. Provide Power Supplies for all exterior PTZ cameras, where required.

2. Shall be dedicated to PTZ cameras, and shall not provide power for fixed cameras or any other low voltage security device.

3. Shall be either rack or wall mount type power supply, as applicable. Provide rack mount power supplies where possible in IDF rooms.

4. Provide sufficient size and quantity of power supplies to allow for a minimum of 20% spare capacity within each individual power supply.

5. Minimum Specifications
    a. Type: UL listed
    b. Input: 120VAC
    c. Output: 24V AC, individually fused and isolated for each camera
    d. Output rating: As required
    e. Enclosure: Steel enclosure with integral lock and tamper switch
    f. Acceptable Manufacturers: Axis, or approved equal

2.08: Network Switches and Associated Network Equipment

A. All network switches provided for the System shall be Power-Over-Ethernet (PoE) type, as required to power the IP Network PoE security cameras.

B. Security Contractor shall provide new PoE Network Switches, as required to fully support all requirements of the Video Surveillance System.

C. Security Contractor shall provide new PoE Switches and commission the Switches, to fully support the new video surveillance system components.

D. Security Contractor shall install, configure, and commission all new security network switches to function as required in conjunction with the video surveillance system equipment.

E. Network Switches and Accessories:

1. Switches are specified and provided as OFE.

2. Contractor shall coordinate with Owner's IT technical staff to assure that the Warranty and Maintenance for the Network Switches are registered in the name of the Owner.

F. Network Patch Panels and Connectors, as required:

1. RJ45 Modular Jacks:

a. Shall be 110Connect type
b. Shall be Category 6 type
c. Shall be compatible with supplied Patch Panels
d. Acceptable Manufacturers: AMP Category 6, or Owner approved equal

2. Patch Panels:
   a. Shall be 110Connect type
   b. Shall be Category 6 type
   c. Shall be compatible with supplied RJ45 Modular Jacks
   d. Acceptable Manufacturers: AMP Category 6, or Owner approved equal

3. RJ45 Connectors:
   a. Shall be Category 6 type
   b. Acceptable Manufacturers: AMP Category 6, or Owner approved equal

4. Shall be provided in IDF rooms by the Telecommunications Contractor. Security Contractor shall coordinate all work with the Telecommunications Contractor.

G. Security Network Back-Bone Cabling, as required:

1. Security switches, NVR's, system server, client workstations, digital video storage devices shall connect and uplink to the Owner's LAN within each local IDF room.

2. Optical Fiber Cabling
   a. As required for riser or horizontal back-bone connectivity between Security Network Switches in MDF and IDF rooms.
   b. Utilize building fiber backbone cabling as required for connectivity. Coordinate specific security system requirements with the Owner and with the Telecommunications Contractor for fiber connectivity locations, and cross-connect patching within MDF and IDF rooms.
   c. Security Contractor shall coordinate all work with the Telecommunications Contractor.
   d. Refer to Division-27 Specifications and Telecommunications Drawings.

3. Copper Cabling
   a. As required for riser or horizontal back-bone connectivity between Security Network Switches in MDF and IDF rooms.
   b. Utilize building copper backbone cabling as required for connectivity. Coordinate specific security system requirements with the Owner and with the Telecommunications Contractor for fiber connectivity locations, and cross-connect patching within MDF and IDF rooms.
   c. Security Contractor shall coordinate all work with the Telecommunications Contractor.
   d. Refer to Division-27 Specifications and Telecommunications Drawings.

3.01: Requirements

A. Refer to Specification Section 28 05 00 Electronic Security Common Work, for Part 3 - Execution requirements.

*****End of Section 28 23 00*****

SECTION 28 31 11 - DIGITAL, ADDRESSABLE FIRE-ALARM SYSTEM

PART 1 - GENERAL

1.1 SCOPE OF WORK

A. This specification provides the requirements for the installation, programming and configuration of a complete Addressable Intelligent Life Safety System for the new Community Building and . The system shall include, but not limited to: Fire Alarm Control Panel, Automatic and Manually activated alarm Initiating and Indicating Peripheral Devices and Appliances, conduit, wire and accessories required to furnish a complete and operational Life Safety System.

1.2 RELATED SECTIONS

A. Section 23000 -- Mechanical

B. Section 26000 -- Electrical

1.3 REFERENCES

A. The equipment and installation shall comply with the current provisions of the following standards:

1. National Electric Code, Article 760.
2. National Fire Protection Association Standards:

    a) NFPA72 National Fire Alarm Code
    b) NFPA101 Life Safety Code

3. Local and State Building Codes.
4. Local Authorities Having Jurisdiction.
5. Underwriters Laboratories Inc.
6. The system and all components shall be listed by Underwriters Laboratories Inc. for use in fire protective signaling system under the following standards as applicable:

a.	UL 864/UOJZ, APOU	Control Units for Fire Protective Signaling Systems.
b.	UL 268	Smoke Detectors for Fire Protective Signaling Systems.
c.	UL 268A	Smoke Detectors for Duct Applications.
d.	UL 217	Smoke Detectors Single Station.
e.	UL 521	Heat Detectors for Fire Protective Signaling Systems.
f.	UL 228	Door Holders for Fire Protective Signaling Systems.
g.	UL 464	Audible Signaling Appliances.
h.	UL 1638	Visual Signaling Appliances.
i.	UL 38	Manually Activated Signaling Boxes.
j.	UL 346	Waterflow Indicators for Fire Protective Signaling Systems.
k.	UL 1971	Standard for Signaling Devices for the Hearing Impaired
l.	UL 1481	Power Supplies for Fire Protective Signaling Systems.
m.	UL 1711	Amplifiers for Fire Protective Signaling Systems.

8. Americans with Disabilities Act (ADA)
9. International Standards Organization (ISO)

a. ISO-9000
b. ISO-9001

1.4 SYSTEM DESCRIPTION

A. The Fire Alarm / Life Safety System supplied under this specification shall be a microprocessor-based network system. All Control Panel Assemblies and connected Field Appliances shall be both designed and manufactured by the same company, and shall be tested and cross-listed as compatible to ensure that a fully functioning Life Safety System is designed and installed.

B. The software shall be windows based. No other OS shall be acceptable.

1.5 SUBMITTALS

A. Submit to the Architect in conformance with the requirements of the Conditions of the Contract: Manufacturer's brochures.

1. Submit to AON/PREI for review.

B. Submit complete manufacturer's specification data sheets on all equipment, devices, and cable to be used in the system.

C. Quality Control Submittals:

1. Letter from manufacturer stating that the Contractor is an Authorized Factory Distributor for the area where the project is located.
2. Current copy of the Contractors license issued by the State Board of Private Investigators.

D. Product Data:

1. Drawing location all components of the security system and indicating circuit routing, cable type, and gauge.
2. Equipment list and data sheets on all security system devices, riser diagrams, special boxes, wire, modules, and other material as requested by the Architect including:

a. Manufacturer.
b. Model Number.
c. Indication all options and accessories.
d. Catalog data sheets with photograph.

E. Submit complete submittal package within 30 calendar days after award of this work for approval. Equipment is not to be ordered without approval.

1.6 PRODUCT DATA

A. The contractor shall submit three (3) complete sets of documentation within 30 calendar days after award of purchase order. Indicated in the documentation will be the type, size, rating, style, catalog number, manufacturers' names, photos, and/or catalog data sheets for all items proposed to meet these specifications. The proposed equipment shall be subject to the approval of the Architect/Engineer and no equipment shall be ordered or installed on the premises without that approval.

B. The Contractor shall provide hourly Service Rates and Semi-Annual inspection prices, performed by a factory trained and authorized personnel, for this installed Life Safety System with the submittal. Proof of that training and authorization of the servicing ESD shall be included in the submittal. These hourly service rates shall be guaranteed for a one-year period unless otherwise specified.

1.7 SHOP DRAWINGS

A. A complete set of Shop Drawings, one for each unit sub-assembly, which requires that a field wire be connected to it, shall be supplied. The Shop Drawings shall be reproduced electronically from a Master Copy supplied by the manufacturer in digital format.

1.8 CLOSE-OUT SUBMITTALS

A. Two (2) copies of the following Manual shall be delivered to the Building Owner's representative at the time of system acceptance. The close out submittals shall include:

1. Operating manuals covering the installed Life Safety System.
2. Point-to-Point diagrams of the entire Life Safety System as installed. This shall include all connected Smoke Detectors and addressable field modules. All drawings shall be provided in CAD and supplied in standard .DXF format. Vellum plots of each sheet shall also be provided. A system generated point-to-point diagram is required to ensure accuracy.
3. The application program listing for the system as installed at the time of acceptance by the building owner and/or Local AHJ (Disk and Hard copy printout).
4. Name, address and telephone of the authorized factory representative.
5. All drawings must reflect device address and programmed characteristics as verified in the presence of the engineer and/or the end user unless device addressing is electronically generated, and graphically printed.

1.9 QUALITY ASSURANCE

A. Qualifications

1. The installing ESD shall provide proof of their qualifications as Factory Authorization and Factory Training for the product(s) specified herein. These qualification credentials shall not be more than two years old, to ensure up-to-date product and application knowledge on the part of the installing ESD.

1.10 WARRANTY

A. Warranty all materials, installation and workmanship for one (1) year from date of acceptance, unless otherwise specified.

B. A copy of the manufacturers' warranty shall be provided with close-out documentation and included with the operation and installation manuals.

1.11 SYSTEM STARTUP, OWNERS' INSTRUCTIONS, COMMISSIONING

A. System startup shall be performed by a Factory Trained and Authorized Engineered Systems Distributor. Certain functions of the Systems Startup Procedure may be performed by a contractor under the direction of the Factory Trained and Authorized Engineered Systems Distributor.

B. The Factory Trained and Authorized Engineered Systems Distributor shall supply owners' Instructions and Operation Manuals at the completion of the project.

C. Commissioning of the installed system shall be performed by the Factory Trained and Authorized Engineered Systems Distributor in the presence of the Local AHJ, the Building Owners' Representative, and a Representative of the General Contractor, if deemed appropriate.

D. A System Generated device map, which will serve as an "as-built" drawing shall be provided to the Local AHJ and the Building Owners' Representative.

PART 2 - PRODUCTS

2.1 ACCEPTABLE MANUFACTURERS

A. The catalog numbers used are those of Edwards Systems Technology (EST), and constitute the type and quality of equipment to be furnished.

B. If equipment of another manufacturer is to be submitted for approval as equal, the contractor shall, at the time of bid, list all exceptions taken to these Specifications, all variances from these Specification and all substitutions of operating capabilities or equipment called for in these Specifications and forward said list to the Engineer. Any such exceptions, variances or substitutions that were not listed at the time of bid and are identified in the submittal, shall be grounds for immediate disapproval without comment. Final determination of compliance with these Specifications shall rest with the Engineer, who, at his discretion, may require proof of performance.

C. Other acceptable manufacturers are; Notifier, Siemens, and Simplex Grinnell.

2.2 CIRCUITING GUIDELINES

A. Each addressable analog loop shall be circuited as shown on the drawings but device loading is not to exceed 80% of loop capacity in order to leave for space for future devices.

B. Where it is necessary to interface conventional initiating devices, provide intelligent input modules to supervise zone wiring.

C. Each of the following types of devices or equipment shall be provided with supervised monitor circuits as shown on the drawings but shall be typically as follows:

1. Sprinkler Water Flow and Valve Supervisory Switches: Provide one (1) supervisory module circuit for each.
2. Kitchen Exhaust Hood Suppression System

D. Each of the following types of remote equipment associated with the fire alarm system shall be provided with a form 'C' control relay contact

1. HVAC Fan Systems: Provide one (1) shutdown control relay contact for each HVAC unit that requires fan shutdown.

2.3 FIRE ALARM SYSTEM SEQUENCE OF OPERATION

A. The system shall identify any off normal condition and log each condition into the system database as an event.

1. The system shall automatically display on the control panel Liquid Crystal Display the first event of the highest priority by type. The priorities and types shall be alarm, supervisory, trouble, and monitor.
2. The system shall have a Queue operation, and shall not require event acknowledgment by the system operator. The system shall have a labeled color coded indicator for each type of event; alarm - red, supervisory - yellow, trouble - yellow, monitor - green. When an unseen event exists for a given type, the indicator shall flash. When all events of a given type have been displayed, the indicator shall change from flashing to steady.
3. For each event, the display shall include the current time, the total number of events, the type of event, the time the event occurred and up to a 40 character custom user description.

    a. The user shall be able to review each event by simply selecting scrolling keys (up-down) for each event type.
    b. New alarm, supervisory, or trouble events shall sound a silenceable audible signal at the control panel.

B. Operation of any alarm initiating device shall automatically:

1. Update the control/display as described.
2. Sound all alarm signals throughout the building at the evacuation rate.
3. Turn on all strobe lights throughout the building.
4. Turn on the red alarm LED at the fire alarm control panel.
5. Operate the alarm relay contacts to initiate the transmission of an alarm to a central station agency via leased telephone lines.
6. Operate control relay contacts to shutdown all HVAC units
7. Operate control relay contacts to release all magnetically held smoke doors throughout the building.
8. Visually annunciate the zone of alarm on the remote annunciator panel where provided. The visual indication shall remain on until the alarm condition is reset to normal.

C. Activation of a sprinkler supervisory initiating device shall:

1. Update the control/display as described above.
2. Turn on the yellow supervisory LED at the fire alarm control panel.
3. Operate the supervisory relay contacts to initiate the transmission of an alarm to a central station agency via leased telephone lines.
4. Visually annunciate the zone of alarm on the remote annunciator panel where provided. The visual indication shall remain on until the supervisory condition is reset to normal.

D. The entire fire alarm system wiring shall be electrically supervised to automatically detect and report trouble conditions to the fire alarm control panel. Any opens, grounds or disarrangement of system wiring and shorts across alarm bell/strobe wiring shall automatically:

1. Update the control/display as described above.
2. Operate the supervisory relay contacts to initiate the transmission of an alarm to a central station agency via leased telephone lines.

3. Visually and audibly annunciate a general trouble condition, on the remote annunciator panel. The visual indication shall remain on until the trouble condition is repaired.

2.4 SUPPORT FOR INSTALLER AND OWNER MAINTENANCE

A. Provide a coded one man walk test feature. Allow audible or silent testing. Signal alarms and troubles during test. Allow receipt of alarms and programmed operations for alarms from areas not under test.

B. Provide internal system diagnostics and maintenance user interface controls to display/report the power, communication, and general status of specific panel components, detectors, and modules.

C. Provide loop controller diagnostics to identify common alarm, trouble, ground fault, Class A fault, and map faults. Map faults include wire changes, device type changes by location, device additions/deletions and conventional open, short, and ground conditions. Ground faults on the circuit wiring of remote module shall be identified by device address.

D. Allow the user to display/report the condition of addressable analog detectors. Include device address, device type, percent obscuration, and maintenance indicator. The maintenance indicator shall provide the user with a measure of contamination of a device upon which cleaning decisions can confidently be made.

E. Allow the user to report history for alarm, supervisory, monitor, trouble, smoke verification, watchdog, and restore activity. Include Facility Name, Licensee, Project Program Compilation date, Compiler Version, Project Revision Number, and the time and date of the History Report.

F. Allow the user to disable/enable devices, zones, actions, timers and sequences. Protect the disable function with a password.

G. Allow the user to activate/restore outputs, actions, sequences, and simulate detector smoke levels.

H. Allow the service user to enter time and date, reconfigure an external port for download programming, initiate auto programming and change passwords. Protect these functions with a password.

2.5 EQUIPMENT

Fire Alarm Control Panel

A. The fire alarm control panels shall be Edwards Systems Technology (EST) type EST2 series and shall incorporate all control electronics, relays, and necessary modules and components in a semi-flush mounted cabinet. The operating controls and shall be located behind locked door with viewing window. All control modules shall be labeled, and all zone locations shall be identified. The cabinet shall be steel, with a gray finish. The assembly shall contain a base panel, system power supply and battery charger with optional modules suitable to meet the requirements of these specifications.

B. System circuits shall be configured as follows: The ability to provide addressable analog loops either Class A Style 7 or Class B; Initiating Device Circuits Class B; Notification Appliance Circuits Class B.

C. The system shall be supervised, site programmable, and of modular design with expansion modules to serve up to 960 detectors and 940 remote modules, and 20 notification appliance circuits (NACs) convertible to power risers to serve remote multiple NAC modules for zoned signal applications.

D. The system shall store all basic system functionality and job specific data in non-volatile memory. The system shall survive a complete power failure intact.

E. The system shall have built-in automatic system programming to automatically address and map all system devices and provide a minimum default single stage alarm system operation with support of alarm silence, trouble silence, drill, lamp test, and reset common controls.

F. The system shall allow down loading of a job specific custom program created by system application software. It shall support programming of any input point to any output point. The system shall support the use of Bar Code readers to assist custom programming functions. It shall allow authorized customization of fundamental system operations using initiating events to start actions, timers, sequences and logical algorithms.

G. The system shall support distributed processor intelligent detectors with the following operational attributes; integral multiple differential sensors, automatic device mapping, electronic addressing, environmental compensation, pre-alarm, dirty detector identification, automatic day/night sensitivity adjustment, dual normal/alarm LEDs, relay bases, and isolator bases.

H. The system shall use full digital communications to supervise all addressable loop devices for placement, *correct location*, and operation. It shall allow swapping of "same type" devices without the need of addressing and impose the "location" parameters on replacement device. It shall initiate and maintain a trouble if a device is added to a loop and clear the trouble when the new device is mapped and defined into the system.

I. The system shall have a UL Listed Detector Sensitivity test feature, which will be a function of the smoke detectors and performed automatically every 4 hours.

J. The system shall support 100% of all remote devices in alarm and provide support for a 100% compliment of detector isolator bases.

K. All panel modules shall be supervised for placement and return trouble if damaged or removed.

L. The system shall have a CPU watchdog circuit to initiate trouble should the CPU fail.

M. The system evacuation signal rate shall be temporal 3-3-3.

N. Provide provisions for a signal silence inhibit feature and an automatic signal silence timer. Audible notification appliances shall be affected by signal silence features.

O. The system program shall meet the requirements of this project, current codes and standards, and satisfy the local Authority Having Jurisdiction.

P. Passwords shall protect any changes to system operations.

Q. The power supply shall be a high efficiency switch mode type with line monitoring to automatically switch to batteries for power failure or brown out conditions. The automatic battery charger shall have low battery discharge protection. The power supply shall provide internal power and 24 Vdc at 4A continuous for notification appliance circuits. The power supply shall be capable of providing 10A to output circuits for a maximum period of 50 ms. Auxiliary power shall be 24 Vdc at 500 mA. All outputs shall be power limited. The battery shall be sized to support the system for 24 hours of supervisory and trouble signal current plus general alarm for 5 minutes.

R. The LCD Display Module shall be of membrane style construction with a 4 line by 20 character Liquid Crystal Display. The LCD shall use supertwist technology and backlighting for high contrast visual clarity. In the normal mode display the time, the total number of active events and the total number of disable points. In the alarm mode display the total number of events and the type of event on display. Reserve 40 characters of display space for user custom messages. The module shall have visual indicators for the following common control functions; AC Power, alarm, supervisory, monitor, trouble,

disable, ground fault, CPU fail, and test. There shall be common control keys and visual indicators for; reset, alarm silence, trouble silence, drill, and one custom programmable key/indicator. Provide four pairs of display control keys for selection of event display by type (alarm, supervisory, monitor and trouble) and forward / backward scrolling through event listings. The operation of these keys shall be integrated with the related common control indicators to flash the indicators when undisplayed events are available for display and turn on steady when all events have been displayed. Allow the first event of the highest priority to capture the LCD for display so that arriving fire fighters can view the first alarm event "hands free". Provide system function keys; status, reports, enable, disable, activate, restore, program, and test. The module shall have a numeric keypad, zero through nine with delete and enter keys.

S. The Main Controller Module shall control and monitor all local or remote peripherals. It shall support the LCD Display Module, power supply, remote LCD and zone display annunciators, strip and carriage printers, and support communication interface standard protocol (CSI) devices such as color computer annunciators and color graphic displays. The RS-485 port shall be capable of supporting up to 32 remote annunciators. The MCM shall provide one loop controller circuit, two notification appliance circuits, and common form 'C' contacts for alarm, supervisory, and trouble. Contact ratings shall be 24Vdc at 1A.

T. The panel shall have provisions for:

1. An Expander Loop Module with one additional loop controller circuit and two notification appliance circuits to expand each panel capability to 192 detectors and 188 modules.
2. A march time module for signal rate control to provide temporal 3-3-3 signal patterns.
3. An interface module for remote site monitoring. The module shall have a local energy municipal loop and reverse polarity connections for each of alarm, supervisory and trouble.
4. A digital alarm communicator transmitter (DACT) module to transmit alarm, supervisory and trouble signals to a Central Monitoring Station (CMS). The DACT shall support dual telephones lines, 20 PPS 4/2 communications, and configured for dual tone multi-frequency (DTMF) or pulse modes. It shall be possible to delay AC power failure reports, auto test call, and site program using a touch tone phone and password.
5. Zone display indicator modules to annunciate zones per the fire alarm zoning schedule.
6. An RS-232 isolator card to isolate grounded peripheral devices (such as printers and CRTs) from the control panel.

2.6 COMPONENTS

A. Remote Booster Power Supplies - General

1. The power supply shall provide a central processor with a watchdog circuit. It shall provide 2 initiating circuits, 2 notification appliance circuits rated at 24 Vdc at 2.5A, form 'C' alarm and trouble contacts, and auxiliary power at 24Vdc at 500 mA. The power supply shall be a high efficiency switch mode type providing 4 A total to the NACs, 500 mA of auxiliary power at 24Vdc, and an automatic battery charger capable of supporting up to 10 AH of sealed lead acid batteries. Site programming shall enable or disable the local trouble buzzer, allow the following of existing signal rates or select internally generated evacuation signal rates at continuous, 20 SPM, 120 SPM, temporal 3-3-3, or California continuous or march time independent of the existing signal rate. Indicators shall be power on, system trouble, ground fault, battery trouble, and notification appliance circuit trouble. It shall be possible to activate the BPS via dry contact or by connection to an existing NAC circuit. It shall be possible to convert the BPS circuits ICs and NACs to Class 'A' operation. The base panel shall provide a communication channel and operating power for expansion modules.

B. Remote Booster Power Supply, BPS

1. The remote booster power supply shall be Edwards Systems Technology (EST) type BPS Series incorporating all control electronics, relays, and necessary modules and components. The panel shall be supervised, site programmable, modular design with expansion modules to serve connection to existing NAC circuits. All initiating, notification, and low voltage power source circuits shall be power limited.

2. The booster power supply shall be provided with battery back up. The batteries shall be of the sealed, lead-acid type and provide twenty-four (24) hours of normal standby operation and five (5) minutes of normal alarm operation at the end of the standby period. The batteries shall be supervised for placement and low voltage. It shall be possible to mount the batteries remote from the panel.

C. Intelligent Detectors -- General

1. The System Intelligent Detectors shall be capable of full digital communications using both broadcast and polling protocol. Each detector shall be capable of performing independent fire detection algorithms. The fire detection algorithm shall measure sensor signal dimensions, time patterns and combine different fire parameters to increase reliability and distinguish real fire conditions from unwanted deceptive nuisance alarms. Signal patterns that are not typical of fires shall be eliminated by digital filters. Devices not capable of combining different fire parameters or employing digital filters shall not be acceptable.
2. Each detector shall have an integral microprocessor capable of making alarm decisions based on fire parameter information stored in the detector head. Distributed intelligence shall improve response time by decreasing the data flow between detector and Analog loop controller. Detectors not capable of making independent alarm decisions shall not be acceptable. Maximum total Analog loop response time for detectors changing state shall be 0.5 seconds.
3. Each detector shall have a separate means of displaying communication and alarm status. A green LED shall flash to confirm communication with the Analog loop controller. A red LED shall flash to display alarm status. Both LEDs on steady shall indicate alarm-standalone mode status. Both LEDs shall be visible through a full 360 degree viewing angle.
4. The detector shall be capable of identifying up to 32 diagnostic codes. This information shall be available for system maintenance. The diagnostic code shall be stored at the detector.
5. Each smoke detector shall be capable of transmitting pre-alarm and alarm signals in addition to the normal, trouble and need cleaning information. It shall be possible to program control panel activity to each level. Each smoke detector may be individually programmed to operate at any one of five (5) sensitivity settings.
6. Each detector microprocessor shall contain an environmental compensation algorithm that identifies and sets ambient “Environmental Thresholds” approximately six times an hour. The microprocessor shall continually monitor the environmental impact of temperature, humidity, other contaminates as well as detector aging. The process shall employ digital compensation to adapt the detector to both 24-hour long term and 4-hour short-term environmental changes. The microprocessor shall monitor the environmental compensation value and alert the system operator when the detector approaches 80% and 100% of the allowable environmental compensation value. Differential sensing algorithms shall maintain a constant differential between selected detector sensitivity and the “learned” base line sensitivity. The base line sensitivity information shall be updated and permanently stored at the detector approximately once every hour.

7. The intelligent Analog device and the Analog loop controller shall provide increased reliability and inherent survivability through intelligent Analog standalone operation. The device shall automatically change to standalone conventional device operation in the event of a loop controller polling communications failure. In the Analog standalone detector mode, the Analog detector shall continue to operate using sensitivity and environmental compensation information stored in

its microprocessor at the time of communications failure. The Analog loop controller shall monitor the loop and activate a loop alarm if any detector reaches its alarm sensitivity threshold.

8. Each Signature Series device shall be capable of automatic electronic addressing and/or custom addressing without the use of DIP or rotary switches. Devices using DIP or rotary switches for addressing, either in the base or on the detector shall not be acceptable.
9. The intelligent Analog detectors shall be suitable for mounting on any Signature Series detector mounting base.

D. Fixed Temperature Heat Detector, SIGA-HFS

1. Provide intelligent fixed temperature heat detectors model SIGA-HFS. The heat detector shall have a low mass thermistor heat sensor and operate at a fixed temperature. It shall continually monitor the temperature of the air in its surroundings to minimize thermal lag to the time required to process an alarm. The integral microprocessor shall determine if an alarm condition exists and initiate an alarm based on the analysis of the data. Systems using central intelligence for alarm decisions shall not be acceptable. The heat detector shall have a nominal alarm point rating of 135°F (57°C). The heat detector shall be rated for ceiling installation at a minimum of 70 ft (21.3m) centers and be suitable for wall mount applications.

E. Photoelectric Smoke Detector, SIGA-PS

1. Provide intelligent photoelectric smoke detectors model SIGA-PS. The analog photoelectric detector shall utilize a light scattering type photoelectric smoke sensor to sense changes in air samples from its surroundings. The integral microprocessor shall dynamically examine values from the sensor and initiate an alarm based on the analysis of data. Systems using central intelligence for alarm decisions shall not be acceptable. The detector shall continually monitor any changes in sensitivity due to the environmental affects of dirt, smoke, temperature, aging and humidity. The information shall be stored in the integral processor and transferred to the analog loop controller for retrieval using a laptop PC <or the SIGA-PRO Signature Program/Service Tool>. The photo detector shall be rated for ceiling installation at a minimum of 30 ft (9.1m) centers and be suitable for wall mount applications. The photoelectric smoke detector shall be suitable for direct insertion into air ducts up to 3 ft (0.91m) high and 3 ft (0.91m) wide with air velocities up to 5,000 ft/min. (0-25.39 m/sec) without requiring specific duct detector housings or supply tubes.
2. The percent smoke obscuration per foot alarm set point shall be field selectable to any of five sensitivity settings ranging from 1.0% to 3.5%. The photo detector shall be suitable for operation in the following environment:

    a. Temperature: 32°F to 120°F (0°C to 49°C)
    b. Humidity: 0-93% RH, non-condensing
    c. Elevation: no limit

F. Standard Detector Mounting Bases, SIGA-SB / SIGA-SB4

1. Provide standard detector mounting bases, SIGA-SB or SIGA-SB4, suitable for mounting on North American 1-gang, 3½" or 4" octagon box and 4" square box. The base shall, contain no electronics, support all Signature Series detector types and have the following minimum requirements:

    a. Removal of the respective detector shall not affect communications with other detectors.
    b. Terminal connections shall be made on the room side of the base. Bases which must be removed to gain access to the terminals shall not be acceptable.
    c. The base shall be capable of supporting one (1) Signature Series SIGA-LED Remote Alarm LED Indicator. Provide remote LED alarm indicators where shown on the plans.

G. Isolator Detector Mounting Bases, SIGA-IB / SIGA-IB4

1. Provide isolator detector mounting bases SIGA-IB or SIGA-IB4 suitable for mounting on <North American 1-gang, 3 ½ " or 4" octagon box and 4" square box. The operation of the isolator base shall be controlled by its respective detector processor. Isolators which are not controlled by a detector processor shall not be accepted. Following a short circuit condition, each isolator/detector shall be capable of performing an internal self-test procedure to re-establish normal operation. Isolator/detectors not capable of performing independent self-tests shall not be acceptable. The isolator base shall support all Signature Series Detector types and have the following minimum requirements:

   a. The isolator shall operate within a minimum of 23 msec. of a short circuit condition on the communication line.
   b. When connected in Class A configuration the Signature Loop Controller shall identify an isolated circuit condition and provide communications to all non isolated analog devices.
   c. Terminal connections shall be made on the room side of the base. Bases which must be removed to gain access to the terminals shall not be acceptable.

H. Detector Mounting Plate, SIGA-DMP

1. Provide detector mounting plate assemblies SIGA-DMP to facilitate mounting a Signature Series detector for direct insertion into a low velocity duct 3 ft (0.91m) high and 3 ft (0.91m) wide, ceiling plenum, or raised floor. Mounting plate shall be code gauge steel with corrosion resistant red enamel finish. The detector mounting plate shall support an intelligent analog detector.

I. Duct Detector Housing, SIGA-DH

1. Provide smoke detector duct housing assemblies SIGA-DH to facilitate mounting an intelligent analog Photoelectric Detector along with a standard, relay or isolator detector mounting base. Provide for variations in duct air velocity between 300 and 4000 feet per minute (300 to 1000 feet per minute for ion-photo-heat detector). Protect the measuring chamber from damage and insects. Provide an air exhaust tube and an air sampling inlet tube which extends into the duct air stream up to ten feet. Provide drilling templates and gaskets to facilitate locating and mounting the housing. Provide five one gang knockouts for mounting optional Signature Series modules. Finish the housing in baked red enamel. Provide Remote Alarm LED Indicators SIGA-LED for each duct detector in ceiling above RTU.

J. Intelligent Modules -- General

1. It shall be possible to address each Intelligent Signature Series module without the use of DIP or rotary switches. Devices using DIP switches for addressing shall not be acceptable. The personality of multifunction modules shall be programmable at site to suit conditions and may be changed at any time using a personality code downloaded from the Analog Loop Controller. Modules requiring EPROM, PROM, ROM changes or DIP switch and/or jumper changes shall not be acceptable. The modules shall have a minimum of 2 diagnostic LEDs mounted behind a finished cover plate. A green LED shall flash to confirm communication with the loop controller. A red LED shall flash to display alarm status. The module shall be capable of storing up to 24 diagnostic codes that can be retrieved for troubleshooting assistance. Input and output circuit wiring shall be supervised for open and ground faults. The module shall be suitable for operation in the following environment:

   a. Temperature: 32°F to 120°F (0°C to 49°C)
   b. Humidity: 0-93% RH, non-condensing

K. Single Input Module, SIGA-CT1

1. Provide intelligent single input modules SIGA-CT1. The Single Input Module shall provide one (1) supervised Class B input circuit capable of a minimum of 4 personalities, each with a distinct operation. The module shall be suitable for mounting on North American 2 ½" (64mm) deep 1-gang boxes and 1 ½" (38mm) deep 4" square boxes with 1-gang covers. The single input module shall support the following circuit types:

    a. Normally-Open Alarm Latching (Manual Stations, Heat Detectors, etc.)
    b. Normally-Open Alarm Delayed Latching (Waterflow Switches)
    c. Normally-Open Active Non-Latching (Monitor, Fans, Dampers, Doors, etc.)
    d. Normally-Open Active Latching (Supervisory, Tamper Switches)

L. Dual Input Module, SIGA-CT2

1. Provide intelligent dual input modules SIGA-CT2. The Dual Input Module shall provide two (2) supervised Class B input circuits each capable of a minimum of 4 personalities, each with a distinct operation. The module shall be suitable for mounting on North American 2 ½" (64mm) deep 1-gang boxes and 1 ½" (38mm) deep 4" square boxes with 1-gang covers. The dual input module shall support the following circuit types:

    a. Normally-Open Alarm Latching (Manual Stations, Heat Detectors, etc.)
    b. Normally-Open Alarm Delayed Latching (Waterflow Switches)
    c. Normally-Open Active Non-Latching (Monitor, Fans, Dampers, Doors, etc.)
    d. Normally-Open Active Latching (Supervisory, Tamper Switches)

M. Monitor Module, SIGA-MM1

1. Provide intelligent monitor modules SIGA-MM1. The Monitor Module shall be factory set to support one (1) supervised Class B Normally-Open Active Non-Latching Monitor circuit. The monitor module shall be suitable for mounting on North American 2 ½" (64mm) deep 1-gang boxes and 1 ½" (38mm) deep 4" square boxes with 1-gang covers.

N. Waterflow/Tamper Module, SIGA-WTM

1. Provide intelligent waterflow/tamper modules SIGA-WTM. The Waterflow/Tamper Module shall be factory set to support two (2) supervised Class B input circuits. Channel A shall support a Normally-Open Alarm Delayed Latching Waterflow Switch circuit. Channel B shall support a Normally-Open Active Latching Tamper Switch. The waterflow/tamper module shall be suitable for mounting on North American 2 ½" (64mm) deep 1-gang boxes and 1 ½" (38mm) deep 4" square boxes with 1-gang covers.

O. Single Input Signal Module, SIGA-CC1

1. Provide intelligent single input signal modules SIGA-CC1. The Single Input (Single Riser Select) Signal Module shall provide one (1) supervised Class B output circuit capable of a minimum of 2 personalities, each with a distinct operation. When selected as a telephone power selector, the module shall be capable of generating its own "ring tone". The module shall be suitable for mounting on North American 2 ½" (64mm) deep 2-gang boxes and 1 ½" (38mm) deep 4" square boxes with 2-gang covers, or European 100mm square boxes. The single input signal module shall support the following operations:

    a. Audible/Visible Signal Power Selector (Polarized 24 Vdc @ 2A, 25Vrms @50w or 70 Vrms @ 35 Watts of Audio)
    b. Telephone Power Selector with Ring Tone (Fire Fighter's Telephone)

P. Dual Input Signal Module, SIGA-CC2

1. Provide intelligent dual input signal modules SIGA-CC2. The Dual Input (Dual Riser Select) Signal Module shall provide a means to selectively connect one of two (2) signaling circuit power risers to one (1) supervised output circuit. The module shall be suitable for mounting on North American 2 ½" (64mm) deep 2-gang boxes and 1 ½" (38mm) deep 4" square boxes with 2-gang covers, or European 100mm square boxes. The dual input signal module shall support the following operation:

    a. Audible/Visible Signal Power Selector (Polarized 24 Vdc @ 2A, 25 Vrms @ 50w or 70 Vrms @ 35w of Audio)

Q. Control Relay Module, SIGA-CR

1. Provide intelligent control relay modules SIGA-CR. The Control Relay Module shall provide one form "C" dry relay contact rated at 2 amps @ 24 Vdc to control external appliances or equipment shutdown. The control relay shall be rated for pilot duty and releasing systems. The position of the relay contact shall be confirmed by the system firmware. The control relay module shall be suitable for mounting on North American 2 ½" (64mm) deep 1-gang boxes and 1 ½" (38mm) deep 4" square boxes with 1-gang covers.

R. Universal Class A/B Module, SIGA-UM

1. Provide intelligent class A/B modules SIGA-UM. The Universal Class A/B Module shall be capable of a minimum of fifteen (15) distinct operations. The module shall be suitable for mounting on North American 2 ½" (64mm) deep 2-gang boxes and 1 ½" (38mm) deep 4" square boxes with 2-gang covers, or European 100mm square boxes. The universal class A/B module shall support the following circuit types:

    a. Two (2) supervised Class B Normally-Open Alarm Latching.
    b. Two (2) supervised Class B Normally-Open Alarm Delayed Latching.
    c. Two (2) supervised Class B Normally-Open Active Non-Latching.
    d. Two (2) supervised Class B Normally-Open Active Latching.
    e. One (1) form "C" dry relay contact rated at 2 amps @ 24 Vdc.
    f. One (1) supervised Class A Normally-Open Alarm Latching.
    g. One (1) supervised Class A Normally-Open Alarm Delayed Latching.
    h. One (1) supervised Class A Normally-Open Active Non-Latching.
    i. One (1) supervised Class A Normally-Open Active Latching.
    j. One (1) supervised Class A 2-wire Smoke Alarm Non-Verified.
    k. One (1) supervised Class B 2-wire Smoke Alarm Non-Verified.
    l. One (1) supervised Class A 2-wire Smoke Alarm Verified
    m. One (1) supervised Class B 2-wire Smoke Alarm Verified
    n. One (1) supervised Class A Signal Circuit, 24Vdc @ 2A.
    o. One (1) supervised Class B Signal Circuit, 24Vdc @ 2A.

S. Isolator Module, SIGA-IM

1. Provide intelligent fault isolators modules SIGA-IM. The Isolator Module shall be capable of isolating and removing a fault from a class A data circuit while allowing the remaining data loop to continue operating. The module shall be suitable for mounting on North American 2 ½" (64mm) deep 2-gang boxes and 1 ½" (38mm) deep 4" square boxes with 2-gang covers, or European 100mm square boxes.

T. Intelligent Manual Pull Stations – General

1. It shall be possible to address each Signature Series fire alarm pull station without the use of DIP or rotary switches. Devices using DIP switches for addressing shall not be acceptable. The manual stations shall have a minimum of 2 diagnostic LEDs mounted on their integral, factory assembled single or two stage input module. A green LED shall flash to confirm communication with the loop controller. A red LED shall flash to display alarm status. The station shall be capable of storing up to 24 diagnostic codes that can be retrieved for troubleshooting assistance. Input circuit wiring shall be supervised for open and ground faults. Pull stations shall be equipped with ST1 Stopper II station protective cover with audible alert. The fire alarm pull station shall be suitable for operation in the following environment:

   a. Temperature: 32°F to 120°F (0°C to 49°C)
   b. Humidity: 0-93% RH, non-condensing

U. Double Action Manual Pull Station, SIGA-278

1. Provide intelligent double action, single stage fire alarm stations. The fire alarm station shall be of lexan construction with an internal toggle switch. Provide a key locked test feature. Finish the station in white with red "PULL IN CASE OF FIRE" lettering. The manual station shall be suitable for mounting on North American 2½" (64mm) deep 1-gang boxes and 1½" (38mm) deep 4" square boxes with 1-gang covers.

V. Beam Type Smoke Detectors, 6424

1. Provide projected beam type smoke detectors. The beam detectors shall be four wire 24 Vdc and powered from the control panel 4 wire smoke power source. This unit shall consist of a separate transmitter and receiver capable of being powered separately or together. This unit shall operate in either a short range of 30 to 100 ft. (9.14 to 30.4 m) or a long range of 100 to 300 ft. (30.4 to 91.4 m). The detector shall feature a bank of four alignment LEDs on both the receiver and transmitter that are used to ensure proper alignment without the use of special tools.
2. The beam detector shall feature automatic gain control which will compensate for gradual signal deterioration from dirt accumulation on lenses. Ceiling or wall mount as shown on the plans. Testing shall be carried out using calibrated test filters.

W. Notification Appliances

1. All appliances shall be UL Listed for Fire Protective Service.
2. All strobe appliances or combination appliances with strobes shall be capable of providing the "Equivalent Facilitation" that is allowed under the Americans with Disabilities Act Accessibilities Guidelines (ADA(AG)), and shall be UL 1971, and ULC S526 Listed.
3. All appliances shall be of the same manufacturer as the Fire Alarm Control Panel specified to assure absolute compatibility between the appliances and the control panels, and to assure that the application of the appliances is done in accordance with the single manufacturer's instructions.

4. Any appliances that do not meet the above requirements, and are submitted for use must show written proof of their compatibility for the purposes intended. Such proof shall be in the form of documentation from all manufacturers that clearly states that their equipment (as submitted) is 100% compatible with each other for the purposes intended.
5. Provide synchronized strobes at the locations shown on the drawings. Strobes shall provide 15cd, 30cd, 60cd, 75cd, or 110cd synchronized flash outputs as required. The light output shall be an even "FullLight" pattern with no hot spots. Strobes using specular reflectors are not acceptable. It shall be possible to flash the strobe at a temporal flash rate. The strobe shall be a low profile design, finished in white and shall not protrude more than 1" off the wall. In-out screw terminals shall be provided for wiring. The strobe shall be suitable for wall mounting and shall mount in a

standard North American 1-gang box. All mounting hardware shall be captive and there shall be no mounting screws visible after the device is installed. The strobes shall be Genesis G1 Series or approved equal as manufactured by EST.

6. Provide synchronized temporal horns at the locations shown on the drawings. The horn shall provide an output of 100 dBA peak using a multiple frequency tone for superior wall penetration. The horn shall be a low profile design, finished in white and shall not protrude more than 1" off the wall. In-out screw terminals shall be provided for wiring. The horn shall be suitable for wall mounting and shall mount in a standard North American 1-gang box. All mounting hardware shall be captive and there shall be no mounting screws visible after the device is installed. The horns shall be Genesis G1 Series or approved equal as manufactured by EST.
7. Provide synchronized temporal horn-strobes at the locations shown on the drawings. Horn-strobes shall provide 15cd, 30cd, 60cd, 75cd, or 110cd synchronized flash outputs. The light output shall be an even "FullLight" pattern with no hot spots. Horn-strobes using specular reflectors are not acceptable. It shall be possible to flash the strobe at a temporal flash rate. Horn and strobe power shall be provided on one pair of wires and terminate on the device on one pair of in-out screw terminals. It shall be possible to independently turn the horn off separately from the strobe. The horn shall provide an output of 100 dBA peak using a multiple frequency tone for superior wall penetration. The horn-strobe shall be a low profile design, finished in white and shall not protrude more than 1" off the wall. In-out screw terminals shall be provided for wiring. The horn-strobe shall be suitable for wall mounting and shall mount in a standard North American 1-gang box. All mounting hardware shall be captive and there shall be no mounting screws visible after the device is installed. The horn-strobes shall be Genesis G1 Series or approved equal as manufactured by EST.

X. Ancillary Devices – General

1. Ancillary devices submitted for use must have written proof of their compatibility for the purposes intended. Such proof shall be in the form of documentation from all manufacturers that clearly states that their equipment (as submitted) is 100% compatible with each other for the purposes intended.

Y. Multi-Voltage Control Relays, MR-100 Series

1. Provide remote control relays connected to supervised ancillary circuits for control of fans, dampers, door releases, etc. Relay contact ratings shall be SPDT and rated for 10 amperes at 115 Vac. A single relay may be energized from a voltage source of 24 Vdc, 24 Vac, 115 Vac, or 230 Vac. A red LED shall indicate the relay is energized. A metal enclosure shall be provided.

Z. Heavy Duty Power Relays, MR-199 Series

1. Provide remote control relays connected to supervised ancillary circuits for control of fans, dampers, door releases, etc. Relay contact ratings shall be DPDT and rated for 30 amperes at 300 Vac or 2 HP motor load. A single relay may be energized from a voltage source of 24 Vac or 115 Vac. A metal enclosure shall be provided.

AA. Electromagnetic Doorholders – General

1. Electromagnetic doorholders submitted for use, when not provided by the Hardware Contractor must have written proof of their compatibility for the purposes intended. Such proof shall be in the form of documentation from all manufacturers that clearly states that their equipment (as submitted) is 100% compatible with each other for the purposes intended.
2. Floor Mounted, 1501/1502 Series
3. Wall Mounted, 1504/1505/1508/1509 Series

BB. Remote LCD Annunciator, LSRA-C

1. Remote alphanumeric annunciators shall be located as indicated on the plans. Each annunciator shall contain a supervised, backlit, liquid crystal display with a minimum of four lines with twenty characters per line. The annuciator shall contain password enabled reset, alarm silence, trouble silence and drill/all call switches.
2. Each annunciator must be capable of supporting custom messages as well as system event annunciation. It must be possible to filter unwanted annunciation of trouble or supervisory functions. The annunciator must incorporate a power saving feature. The front panel back lighting must turn off after a minimum of four minutes if there is no switch activity and no unacknowledged messages waiting.

The entire system shall be installed in a skillful manner in accordance with approved manufacturers' manuals and wiring diagrams. The contractor shall furnish all conduit, wiring, outlet boxes, junction boxes, cabinets and similar devices necessary for the complete installation. All wiring shall be of the type recommended by the NEC, approved by local authorities having jurisdiction for the purpose, and shall be installed in dedicated conduit throughout.
All penetration of floor slabs and fire walls shall be fire stopped in accordance with all local fire codes.
End of Line Resistors shall be furnished as required for mounting as directed by the manufacturer.
All wiring shall be installed according to NEC standards per the drawings submitted by the authorized Engineered Systems Distributor, unless otherwise noted.

PART 3 - EXECUTION

3.1 FIELD QUALITY CONTROL

A. The system shall be installed and fully tested under the supervision of trained manufacturer's representative. The system shall be demonstrated to perform all the functions as specified.

3.2 ACCEPTABLE INSTALLERS

A. The Fire Alarm / Life Safety System specified herein shall be installed by a Factory Trained and Authorized Engineered Systems Distributor, such as Lone Star Communications, Inc.

3.3 INSTALLATION

A. The Smoke detectors will be required in the corridors. They will be “hardwired” into the low voltage wiring. The smoke detectors will be addressable. Smoke alarms will be required in the units. Within a dwelling unit each bedroom should have a smoke alarm and each hallway to a bedroom should have a smoke alarm. This means multiple smoke alarms in the larger units for each bedroom (and hallway). The smoke alarms should be multiple-station (interconnected to each other within the same dwelling unit). The smoke alarms within the units should be hardwired with 120 V service. Unit smoke alarms shall be tied to the E-Call System. Basis of Design: Gentex 9120F

3.4 EXAMINATION

A. Prior to the commencement of any of the work detailed herein, an examination and analysis of the area(s) where the Fire Alarm / Life Safety System and all associated components are to be installed shall be made.

B. Any of these area(s) that are found to be outside the manufacturers' recommended environments for the particular specified products shall be noted on a Site Examination Report which shall be given to the Building Owners' Representative, and the local AHJ.

3.5 DEMONSTRATION

A. Each of the intended operations of the installed Fire Alarm / Life Safety System shall be demonstrated to the Building Owners' Representative and the Local Authority Having Jurisdiction by the Installing ESD.

END OF SECTION 28 31 11