USC GUIDELINE SECURITY SPECIFICATIONS

TABLE OF CONTENTS

END OF TABLE OF CONTENTS

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 27 32 26
EMERGENCY PHONE SYSTEM

PART 1 GENERAL

1.1 DESCRIPTION

A. This specification section covers the furnishing and installation of Emergency Phones at [Indicate Site and Building].

B. Security Integrator shall furnish and install hardware devices, mounting brackets, power supplies, switches, controls, and other components of the system as shown and specified.

C. Licensed Electrical Contractor shall Furnish and install outlets, junction boxes, conduit, connectors, wiring, and other accessories necessary to complete the system installation. Requirements shall be in accordance with Division 26, Electrical.

1.2 PRECEDENCE

Obtain, read and comply with General Conditions and applicable sub-sections of the contract specifications. Where a discrepancy may exist between any applicable sub-section and directions as contained herein, this section shall govern.

1.5 GENERAL CONDITIONS

In accordance with Section 28 05 00, Security System General Requirements

1.6 RELATED WORK

A. In accordance with Section 28 05 00, Security System General Requirements

B. In accordance with Section 28 07 00, Security System Integration

C. In accordance with Section 28 08 00, Security System Testing and Commissioning

1.7 APPLICABLE PUBLICATIONS

In accordance with Section 28 05 00, Security System General Requirements

1.8 SHOP DRAWINGS & EQUIPMENT SUBMITTAL

In accordance with Section 28 05 00, Security System General Requirements

1.9 OPERATING AND MAINTENANCE MANUALS

In accordance with Section 28 05 00, Security System General Requirements.

1.10 SERVICE AND MAINTENANCE

In accordance with Section 28 05 00, Security System General Requirements

1.11 TRAINING

In accordance with Section 28 05 00, Security System General Requirements

1.12 WARRANTY

In accordance with Section 28 05 00, Security System General Requirements

1.13 TECHNICAL REQUIREMENTS, EMERGENCY PHONE SYSTEM

A. General

1. The following information is provided to establish required system performance for a complete operating Emergency Phone System for [Indicate Site and Building]. Some functions and performance requirements noted herein are supported and supplied by existing systems in concert with new equipment which shall be provided by the Contractor under this scope of work. Contractor shall provide

equipment, wiring and programming at all sites as necessary to provide a complete system as described herein and as shown on the drawings.

2. Components provided under this scope of work shall be compatible with the USC communications phone system and connected to the EACS portion of this project.
3. Contractor shall be responsible for providing equipment and connections to achieve specified system performance.

B. Purpose: The system is designed to allow communications from the device to the programmed responding location allowing the responder to assist the caller.
   1. Attributes
      a. General
         1) Exterior Emergency phones with visual locating devices are located in public areas outside the buildings as shown on plans.
         2) *[Emergency phones are located in areas of refuge identified on the plan drawings.]*
      b. Exterior Emergency Phones
         1) Emergency phones utilize the campus phone system dialing automatically to call a monitoring location.
         2) Each device shall be equipped with a blue light identifying the location of activation.
         3) Each device shall be equipped with an Axis CCTV camera for situational overview.
         4) Each device shall be equipped with a single pushbutton which will activate the calling function and the blue location light.
         5) Emergency phone shall be provided in a wall mounted or free standing configuration, as indicated on the plans.
         6) Enclosures and equipment shall be weatherproof, and specifically rated for exterior use.
      c. Interior Emergency Phones
         1) Emergency phones utilize the campus phone system dialing automatically to call a monitoring location.
         2) Each device shall be equipped with a blue light identifying the location of activation.
         3) Each device shall be equipped with an Axis CCTV camera for situational overview.
         4) Each device shall be equipped with a single pushbutton which will activate the calling function and the blue location light.
         5) Emergency phone shall be provided in a wall mounted configuration, as indicated on the plans.

PART 2 PRODUCTS

2.1 GENERAL

A. Product Acceptability: The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified and compatible with the existing USC system.

Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified. Contractor may not use contractor proprietary interface modules for connections between field devices and controller

B. Equipment shall have a UL Listed mark on the product.

C. Assemblies shall be approved by a recognized agency acceptable to the City of Los Angeles.

2.2 EMERGENCY PHONE

A. Provide Emergency Phones in the following configurations. Phones shall incorporate communication compatible with the Owner's communications system.

1. Exterior Tower Phone
    a. Provide "Talk-A–Phone" model ETP-MTE-72 -Eco Tower, with the following characteristics.
        1) ETP-MTE-WP-ARM for CCTV and WAP mounting points.
        2) Axis CCTV Camera mounted to CCTV arm.
        3) Vandal-resistant, exterior enclosure.
        4) Blue Strobe Light housed in protective acrylic housing that is activated when the call button is pressed
        5) Constant light Faceplate
        6) [Indicate low voltage version where required by project] Low voltage version shall be 24VDC.
        7) Provide color as required by Owner [Color: Chilean Red]
        8) Shall meet ADA requirements for access
        9) UL listed
    b. Provide ETP-500C single button faceplate with Red Emergency activation button
        1) LED indicator for hearing impaired
        2) Built in auto-dialer
        3) Auto-Answer
        4) Second number dial on first number no answer
        5) Unit shall be handsfree after activation
        6) Stainless Steel faceplate
        7) Shall include speaker for audible communication
        8) Shall include activation button.
2. Exterior Wall Phone
    a. Provide "Talk-A–Phone" model ETP-WM Phone
        1) [Indicate flush or surface mounting] Vandal-resistant
        2) Blue Light housed in protective acrylic housing
        3) Activated Strobe light when call button is pressed
        4) Constant light Faceplate
        5) [Indicate low voltage version where required by project] Low voltage version shall be 24VDC.
        6) Axis CCTV Camera mounted above on wall.
        7) Provide color as required by Owner
        8) UL listed

b. Provide “Talk-A–Phone” model ETP-500C single button faceplate with Red Emergency activation button
   1) LED indicator for hearing impaired
   2) Built in auto-dialer
   3) Auto-Answer
   4) Second number dial on first number no answer
   5) Unit shall be handsfree after activation
   6) Stainless Steel faceplate
   7) Shall include speaker for audible communication
   8) Shall include activation button

3. Interior Wall Phone
   a. Provide “Talk-A–Phone” model ETP-400C Phone
      1) Stainless Steel faceplate
      2) Single push button activation
      3) LED indicator for hearing impaired
      4) Built in auto-dialer
      5) Auto-Answer
      6) Second number dial on first number no answer
      7) Axis CCTV Camera mounted above on wall.
      8) UL listed
   b. Provide [indicate] surface / flush mounting enclosure to match phone.

2.3 WIRE AND CABLE

A. General: Cables which are not installed in conduit shall be a version of the specified cable rated for use in plenums.

B. System cable: Provide cable as shown below, or as recommended by the Manufacturer.
   1. Emergency Phone: Belden 5302GE, 1 Pair Twisted Shielded 18AWG, with 2 conductor 18AWG, or equal.
   2. Alarm Monitoring: Belden 5500FE, 1Pair Shielded 22AWG, or equal, for conection to EACS.
   3. Network Cable: As required by Owner Infrastructure.

C. Cable installed below grade shall be rated for immersion in water.

PART 3 EXECUTION

3.1 GENERAL

In accordance with Section 28 05 00, Security System General Requirements.

3.2 EMERGENCY PHONE INTEGRATION

A. Provide access control system integration equipment, software programming, in accordance with Section 28 07 00, Security System System Integration. In addition provide specific integration schemes noted.

3.3 GROUNDING PROCEDURES

Provide grounding of all systems and equipment in accordance with Section 28 05 00, Security System General Requirements.

3.4 WIRE AND CABLE INSTALLATION PRACTICES

Provide wire and cable installation in accordance with Section 28 05 00, Security System General Requirements.

3.5 START-UP RESPONSIBILITY

Provide start-up services for all systems and equipment in accordance with Security System General Requirements, Section 28 05 00.

3.6 PRELIMINARY INSPECTION AND TESTING

Provide preliminary inspection and testing services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

3.7 SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

A. Provide performance testing and adjusting of systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

B. Emergency Phone
   1. Verify phone indicator is on
   2. Verify phone indicator flashes when activated.
   3. Verify voice communication with called station
   4. Verify visual indicator is on during normal operation
   5. Verify visual indicator strobe function is activated during use.

3.8 BURN-IN PERFORMANCE PERIOD

Provide a burn-in performance period to demonstrate the stability of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.9 COMMISSIONING AND VALIDATION

Provide commissioning and validation services to prove and improve the effectiveness of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.10 TRAINING

A. Provide training requirements of Security System General Requirements Section 28 05 00

3.11 FINAL PROCEDURES

Perform final procedures in accordance with section 28 05 00, Security System General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 05 00
SECURITY SYSTEMS GENERAL REQUIREMENTS

PART 1 GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and other Division 01 Specification Sections, apply to this Section.

1.2 BASIC DEFINITIONS

A. The University of Southern California (USC) shall be hereinafter referred to in this document as Owner and the respondent shall be referred to as Contractor. The term Owner includes direct employees and other appointed Owner agents such as Architects or consultants. These agents may be requested by Owner to represent Owner in undertaking certain project tasks.

B. "Days": As used in the specifications, the word "days" means calendar days including weekend days.

C. "Provide": As used in the plans and specifications, the word "provide" means to furnish, install, connect, program, test, commission and warranty the subject material or services.

D. Specified Items - Substitutions

1. "No Acceptable Equal": The exact make and model number identified in this Specification shall be provided without exception. Where compatibility with existing systems is specified, and where a specific make or model number is not identified, the Security Integrator shall provide equipment which is compatible with, and equivalent to, existing equipment of the same description and type, and serving the same purpose.
2. "Or Equal": An item may be substituted for the specified item provided that in every technical and aesthetic sense, the substituted item provides the same or better capability than the specified item, and is fully compatible with the new or existing systems specified. For expansion of existing systems, the item shall also be approved and fully supported by the existing system manufacturer. The Owner shall be the sole authority to determine the equality of substituted products with specified items.
3. "Aesthetics", or "Aesthetic Considerations": If aesthetic considerations are involved in either the `or equal' or `approved equal' category, this shall be a consideration in approving or disapproving the proposed substitute. If the proposed substitute is aesthetically unacceptable to the Owner, then the specified, or another technically equal item, shall be provided.

E. "Beneficial Use": Each component of a system is not considered available for beneficial use until and unless all components and conditions have been fulfilled to make the system fully operational.

1.3 LOCATION AND ACCESS TO PROJECT

A. Project is located at the [Indicate Site and Building].

B. Any access using normal highway routing to the facility is acceptable.

C. Permission for access to this campus or facility may be revoked for any and all persons who violate facility traffic regulations including speed limits, parking restrictions and directions of the responsible Owner or project personnel. Contractor's personnel, operating forces, and delivery personnel shall be made aware of and shall comply at all times with the regulations and the direction of responsible Owner and project personnel.

1.4 SITE ACCESS CONTROL

A. The Contractor shall obtain rules and regulations from the Owner and shall train construction and delivery personnel on their requirements. Contractor shall consistently remain in contact with the Architect for revisions to project policy and shall be held fully responsible for monitoring and ensuring Contractor and Subcontractor compliance to USC Access Control rules and regulations as directed by the Architect.
B. Contractor's personnel, operating forces, and delivery personnel shall strictly follow all rules and regulations concerning Access Control at the University, including but not limited to those relating to credentialing, background checks, and access to restricted and secure areas, parking, the handling of Access Control information, and the use of the facility.

1.5 DESCRIPTION

A. General Description: This specification section covers general requirements for the furnishing, installation, and testing of a complete expansion to the Owner's electronic access control, electronic intrusion detection system, and video surveillance system.
B. Furnish and install Electronic Access Control System (EACS) software programming, hardware devices, mounting brackets, power supplies, switches, equipment cabinets, controls, consoles, and other components of the system as shown and specified.
C. Furnish and install intrusion detection and duress system devices and Electronic Intrusion Detection System (EIDS) transmitter panel, as shown and specified.
D. Furnish and install Video Surveillance System (VSS) software programming, hardware devices, mounting brackets, power supplies, video servers, Genetec Archivers, and equipment enclosures, as shown and specified.
E. Furnish and install outlets, junction boxes, pull boxes, conduit, connectors, wiring, and other accessories necessary to complete the system installation. Requirements shall be in accordance with Division 26, Electrical Work.

1.6 EXISTING SYSTEMS AND SUBSYSTEMS

A. Electronic Access Control System (EACS)
    1. The primary system for centrally managed physical access control within USC is the OnGuard System, manufactured by Lenel Systems International (Lenel). The deployed card readers are proximity/multi-technology card readers, compatible with USCard credentials and supported by the EACS. The system generally comprises a wide-area data network, enterprise server, enterprise administrative and monitoring clients, communications client, remote system controllers, and card readers compliant with the campus credentialing system.
    2. The system operates seamlessly with the USCard credentialing system, sharing appropriate records of the Credentialing database to support the control of physical access. New work shall maintain this integration.
    3. The Lenel OnGuard system will be integrated with a Genetec Video surveillance system (VSS), to provide automatic call-up and pre-positioning of cameras associated with alarm and emergency event activity. New devices installed as part of this work must replicate this level of integration.
    4. Modifications to the existing USC EACS System
        a. The Security Integrator shall use and expand, as necessary, the existing Lenel system as part of this work, including but not limited to the addition of servers, workstations, input/output modules, control keyboards, computers, software, software licensing for new equipment, system programming, wiring, and system controllers.

b. Contractor shall subcontract with the Owner's EACS service and maintenance providers to ensure new and modified systems are fully and seamlessly integrated into the existing system.
c. Not used.
d. The system shall support existing HID, XceedID and AptiQ proximity card readers and card population.

B. Credentialing System
1. The existing system is designed to provide credentials for USC staff, students, contractors/vendors, support, and administrative personnel. The credential is used for access control, as well as numerous other campus services requiring identity validation.
2. The system is currently managed by the USCard Services department. Appropriate fields of the credentialing system database are automatically created on the EACS for use in access control configuration.
3. Modifications to the existing credentialing system are not a part of this work.

C. Video Surveillance System (VSS)
1. Genetec Digital Video System
a. The primary system for recording and monitoring campus cameras is the digital video surveillance system manufactured by Genetec. The system provides visual monitoring of strategic areas of USC campus grounds and/or facilities, and is entirely LAN network-based, using TCP/IP devices, digital recording media, network video archivers and "virtual" switching/viewing software.
b. Command and Control: The system is monitored and managed from the Department of Public Safety (DPS) Police Dispatch Center, via VSS workstations and the appropriate viewing software. Connectivity is made via the campus Local Area Network (LAN).
c. The VSS system is integrated with the access control system (Lenel OnGuard PRO-I Edition) to provide automatic call-up, real-time recording, and prepositioning of cameras associated with alarm and detection events.
2. Modifications to the Existing System
a. The Genetec expansion shall be fully integrated with the existing Genetec system located at the University Park Campus, and shall provide services and functions identical to the existing system in addition to any new functions and services specified herein.
b. Local Monitoring and Control: The system may be monitored by any suitably configured computer workstation with the appropriate Genetec viewing client software that is added by this project.
c. The Security Integrator shall use and expand, as necessary, the existing system as part of this work, including but not limited to servers, encoders, recorders, input/output modules, control keyboards, workstations, software, software licensing, wiring, cameras, and appurtenances.
d. The Security Integrator shall coordinate with the USC Administrative Operations Department to ensure new and modified systems are fully and seamlessly integrated into the existing system.
e. The Security Integrator shall coordinate with the Owner's service and maintenance providers to ensure new additions and modified systems are fully and seamlessly integrated into the existing system.

D. The Security Integrator and Manufacturer shall guarantee in writing equipment and software which is added as part of this work is fully compatible with the existing system, is fully supported by the existing system manufacturer(s), and is

configured as described in the specifications. New equipment shall be fully warranted by the Security Integrator as specified herein.

E. The Security Integrator shall ensure hardware and software is fully integrated into the existing system to present a single, seamless operating system. The Security Integrator shall fully develop and support all hardware and software integration schemes.

F. Control components which require unique, or proprietary, hardware or software interfaces to achieve parity with the existing system architecture are not acceptable.

G. If records exist, drawings and diagrams of the existing systems will be made available, through the Owner, to the Contractor. The Security Integrator shall survey, research, and confirm the existing equipment and configuration in-place, and coordinate expansion of the systems with the Owner to avoid any interruption in services.

H. The Security Integrator shall guarantee the existing equipment and software, including (user programming, cardholder, and tenant databases) shall be protected from corruption or damage during the installation, programming, and commissioning process.

1.7 SCOPE OF WORK

A. Systems: Provide an Electronic Access Control System (EACS) expansion to the Lenel system, a Video Surveillance System (VSS) expansion of the Genetec system, and Electronic Intrusion Detection System (EIDS) complete per the contract schedule, and with acceptable engineering and installation practices as described herein.

B. Areas of work include, but are not limited to:
   1. [Indicate Site and Building]

C. Services: The Security Integrator shall provide the following services complete and as scheduled:
   1. Project Planning and Management
   2. Shop Engineering and Documentation
   3. Wiring and Installation Diagrams
   4. Submittals
   5. Coordination
   6. System Installation
   7. System Integration
   8. Training
   9. Start-up Testing
   10. Commissioning
   11. Close out As-Built documentation
   12. Warranty

1.8 BID RESPONSE

A. Bidders Responsibility
   1. The Security Integrator is responsible for verifying actual conditions by visiting the site, reviewing the Specifications and drawings, and to advise the Owner in writing of any conditions which may adversely affect the work. If any necessary exceptions are discovered, the Security Integrator shall immediately notify the Owner for resolution prior to any change in the design or the scope, and any resultant claim for additional compensation.
   2. The Bid Response must fulfill the intent of the Drawings and Specifications to the satisfaction of the Owner to qualify as an acceptable Bid Response.

B. Substitutions
   1. Catalog and/or model numbers for Owner approved equipment and systems are included as a part of these specifications.

2. Any substitution proposed by the Security Integrator for catalog numbers and brands or trade names noted or specified herein shall be solely at the Security Integrators risk. The Owner maintains sole authority to hold a review of substitutions, and sole authority to approve or disapprove of substitutions for any reason.
3. The Owner's acceptance of substitutions shall not relieve the Security Integrator from complying with the requirements of the drawings and Specifications. The Security Integrator shall be responsible, at the Security Integrator's sole expense, for any changes resulting from the Security Integrator's substitutions that affect other parts of Contractor's own work or the work of others.

C. Technical Bid Submission: At bid submission, submit one (1) copy of the following
1. An equipment list with names of Manufacturers of primary systems (EACS, VSS and EIDS,) including model numbers and technical information on equipment proposed.
2. A letter from the manufacturer(s) stating that the system Security Integrator is an authorized distributor or installer of the proposed primary systems (EACS, VSS and EIDS).
3. Indicate complete and total compliance with the provisions of these Specifications by letter or by submittal of the bid response forms, signed by an officer of the corporation, or a principal if other ownership currently exists. If there are exceptions to the specifications, submit a statement listing every technical and operational parameter wherein the submitted equipment or system may vary from that which was originally specified. If the submitter fails to list a particular variance and their submittal is accepted, but is subsequently deemed to be unsatisfactory because of the unlisted variance, the submitter must replace or modify such equipment at once and without cost to the Owner.
4. Failure of the Security Integrator to submit the above information shall be considered nonresponsive to the bid requirements and sufficient cause for bid rejection.

D. Examination of Site and Verification of Existing Conditions
1. The Security Integrator shall have visited the site and familiarized themself with existing conditions prior to submitting their bid and shall be prepared to carry out the work within the existing limitations. Failure or neglect to do so shall not relieve the Security Integrator of their responsibilities nor entitle them to additional compensation for work overlooked and not included in their bid.
2. Existing structures and utilities shown on the contract drawings are obtained from project drawings and exploratory field examination. The Security Integrator shall verify existing conditions and required dimensions, including those shown on the drawings, by measurement at the job site. The Security Integrator shall notify the Owner of exceptions before proceeding with the work.
3. The Security Integrator shall confirm the availability of the proper power source for each piece of specified equipment, through site visits and drawings, as necessary. Where proper power does not exist, Contractor shall identify this situation to the Owner for guidance. Should the Owner direct Contractor to provide the necessary power, it shall be provided using equipment and methods authorized by the Owner.

E. Data Accuracy: Absolute accuracy of information regarding existing conditions cannot be guaranteed. The Drawings and Specifications are for the assistance and guidance of the Security Integrator and exact locations, distances, and elevations

will be governed by actual field conditions. Where variations from the bid documents are required, such variations shall be approved by the Owner.

1.9 QUALIFICATIONS

A. General
   1. The approved Security Integrator shall be responsible for satisfactory operation of the system and its certification.
   2. Approval of the Owner is required of products or services of the proposed manufacturer, suppliers and installers and will be based upon conformance to the specifications.

B. Manufacturer Qualifications
   1. System components shall be furnished by manufacturers of established reputation and experience who shall have produced similar equipment and who shall be able to refer to similar installations rendering satisfactory service.
   2. The manufacturer's products shall have been in satisfactory operation on at least three similar installations for not less than three years. The Security Integrator shall submit a list of similar installations.
   3. Components including, but not limited to, card access controllers, cameras, intercoms, computers, and power supplies shall have been tested and listed by Underwriters Laboratories, Inc., Factory Mutual Systems, or another approved independent testing laboratory.
   4. Components installed within a common enclosure shall be approved by an agency recognized by the City of Los Angeles Department of Building and Safety as an assembly.

C. Security Integrator Qualifications for Security Systems
   1. The Security Integrator shall be a pre-qualified supplier of USC purchasing, Facility Management Services and Career and Protective Services (CAPS) departments.
   2. Hold current legally required California State Contractor's licenses necessary to accomplish the installation and activation of the described system at the facilities indicated. The Security Integrator shall submit copies of licenses to Owner prior to the start of work.
   3. Hold current legally required state registrations required to meet local requirements for submittal drawings.
   4. Have manufacturers trained and certified engineering, field technicians and programming staff.
   5. Indicate complete and total compliance with the provisions of these Specifications by letter or by submittal of the bid response forms, signed by an officer of the corporation, or a principal if other ownership exists. In addition, the letter or forms shall include a complete listing of exceptions, if any.

1.10 GENERAL CONDITIONS

A. Contract Compliance: Provide the Systems and Services in accordance with the conditions and system descriptions as described in Part 1 of each specification section. Provide specified or Owner approved equivalent alternate products as described in Part 2 of each specification section. Utilize specified procedures and practices as described in Part 3 of each specification section.

B. Codes: Furnish material and workmanship for this work in conformance with applicable legal and code requirements.

C. Inclusive Work: Provide sufficient time, material and manpower to verify, revise or refine the Bid Drawings as necessary to develop fully engineered Shop Drawings as required by the General Requirements, and in order for this work to realize complete, stable and safe operation.

1.11 RELATED WORK

A. General
   1. Observe interface procedures to related work.
   2. Coordinate with the Owner on aspects of aesthetic interface.
   3. Coordinate this work with related work by other contractors.
   4. Coordinate with existing construction, equipment, and field devices.
   5. Equipment provided under this project shall be installed in a manner consistent with architectural, operational, service, and maintenance considerations.
   6. Coordinate related work not specifically mentioned below.

B. Owner's General Provisions and Work Contract

C. Division 01, General Requirements: Coordinate this work with applicable sections of the Owner's General Requirements and General Provisions.

D. Division 08, Openings: Coordinate this work with applicable sections of Division 08, Openings, including but not limited to the following.
   1. Schedules for Openings: Coordinate Access Control requirements with door, frame, and hardware schedules.
   2. Section 08 71 00 – Hardware, and the University guidelines for door hardware.
   3. Door hardware, door and frame modifications shall be provided by the Contractor. Contractor shall coordinate with the Owner on requirements and interfaces with Access Control hardware.
   4. Access Doors: Coordinate with the Owner for the provision of access doors where needed to gain access to wiring, boxes, panels and enclosures in walls or ceilings.

E. Finishes: Coordinate this work with applicable Owner requirements for Finishes, including but not limited to the following.
   1. Painting/Patching: Provide painting, patching, and repair services to match existing conditions.
   2. Painting of walls shall be from corner of nearest wall across repair area to nearest wall on opposite side of repair area.

F. Division 14, Conveying Equipment: Coordinate this work with applicable Owner requirements of, Conveying Equipment, including but not limited to the following.
   1. Owners requirements for Elevator Equipment and Controls
      a. Elevator work shall be provided by the Owners Contractor.
   2. Contractor shall coordinate with the Owner on requirements and interfaces with elevator equipment.

G. Division 26, Electrical
   1. Coordinate this work with applicable sections of Division 26, Electrical, including but not limited to the following.
   2. Electrical power distribution sources for existing buildings shall be by the Owner unless otherwise noted. Contractor shall coordinate with the Owner to identify and verify 120-volt power service requirements with the first shop drawing submittal.
   3. Conduit, boxes, and rough-in material shall be provided and installed by the Contractor, unless otherwise noted.
   4. Specialty boxes shall be provided by the Contractor and installed by the Contractor, unless otherwise noted.

H. Division 27, Communications

1. General: Coordinate this work with applicable sections of Division 27, Communications, including but not limited to structured cabling, fiber optic cabling. telephone, and data communications requirements.
2. Contractor shall coordinate with the Owner to identify and verify shared cable/pathway, LAN ports, and bandwidth requirements at the time of the first shop drawing submittal.

I. Division 28, Electronic Safety and Access Control
1. Existing Systems: Coordinate with Owner and Owner's existing Service Provider to ensure the existing system(s) are kept in active operation during the course of this project, in keeping with appropriate phases of work. Coordination may require reconfiguration and reprogramming of existing controllers and other system elements. This work will be coordinated by the Contractor and provided by the Owner or an Owner-selected Service Provider.
2. Section 28 05 00 – Security System General Requirements
   a. Provide equipment and services required by related Sections pursuant to the requirements of Section 28 05 00, Security System General Requirements.
3. Section 28 05 53 – Identification for Electronic Safety and Security
   a. Provide equipment and services required by related Sections pursuant to the requirements of Section 28 05 53, Identification for Electronic Safety and Security.
4. Section 28 07 00 – Security System Integration
   a. Provide equipment and services required by related Sections pursuant to the requirements of Section 28 07 00, Access Control System Integration.
5. Section 28 08 00 – Testing and Commissioning
   a. Provide equipment and services required by related Sections pursuant to the requirements of Section 28 08 00, Testing and Commissioning.
6. Section 28 13 00 - Electronic Access Control System
   a. Provide equipment and services required by Section 28 13 00, Alarm and Access Control System, pursuant to the requirements of this section.
7. Section 28 16 00 - Electronic Intrusion Detection System
   a. Provide equipment and services required by Section 28 16 00, Electronic Intrusion Detection System, pursuant to the requirements of this section.
8. Section 28 23 00 - Video Surveillance System
   a. Provide equipment and services required by Section 28 23 00, Video Surveillance System, pursuant to the requirements of this section.

J. Coordinate related work with door hardware including but not limited to automatic motorized door opening, power assisted door opening and powered panic hardware.

1.12 PRECEDENCE

A. If any statement in this or any other Access Control specification conflicts with any provision of the General Terms and Conditions of the contract, the provision stated in the General Terms and Conditions shall take precedence. Any questions that result from such potential conflict, which require additional interpretation and guidance shall be immediately brought to the Owner's attention.

B. Obtain, read, and comply with Division 26, Electrical and applicable sub-sections of the contract specifications. Where a discrepancy may exist between any applicable Division 26 sub-sections and directions as contained herein, this section shall govern.

C. Architectural drawings shall have precedence over other drawings regarding dimensions and location.

1.13 APPLICABLE PUBLICATIONS

A. The edition of the appropriate code or standard at the time of permitting shall govern all applications.

B. Standards: Perform the work in accordance with the following standards:

1. UL - Underwriters Laboratories, Inc., UL 294, UL 1076, ULC
2. EIA - Electrical Industries Association.
3. NTSC - National Television Standards Committee.
4. NEMA - National Electrical Manufacturers Association.
5. NECA - National Electrical Contractors Association, Standards of Installation.
6. NFPA - National Fire Protection Association 101 Life Safety Code
7. CCR Title 24 California Building Code
8. CCR Title 24 California Electric Code
9. ADA - Americans With Disabilities Act
10. FCC Part 15, Part 68
11. IEEE RS 170 variable standard NTSC (color camera broadcast)
12. OSHPD - Office of State Health Planning Department

C. Where more than one code or regulation is applicable, the more stringent shall apply.

D. Cable installation, identification and termination shall be performed in accordance with manufacturer's installation manuals in addition to the above applicable codes.

E. In the absence of manufacturer's recommendations on conductor applications, the Contractor shall ensure that the cable selected meets all technical requirements of the location of its installation, and of the equipment to be installed.

1.14 SHOP DRAWING & EQUIPMENT SUBMITTAL – SECURITY SYSTEMS

A. General: Bid documents, including drawings, details and specifications are considered conceptual in nature, and provide direction on products and project requirements. The Security Integrator is given a choice of methods that may be incorporated into the system. These choices may affect the overall design, configuration, and installation of the proposed system.

B. Security Integrator Responsibility: Prepare and submit shop drawings, rendered in the latest AutoCAD format, which show details of all work to ensure proper installation of the work using those materials and equipment specified or allowed under the approved plans and specifications. A complete Shop Drawing submittal package shall consist of Drawings, Equipment Data Sheet Submittals, and an Acceptance Testing Plan.

C. Completeness: The Equipment Submittals, Acceptance Testing Plan and the Shop Drawings should be submitted as a complete and contiguous package. Partial or unmarked submittals will not be accepted for review.

D. Scheduling: A schedule of shop drawing submissions shall be submitted for the Owner’s review on a form acceptable to the Owner within ten (10) days after award of the Contract. The schedule of shop drawing submissions shall include as a minimum, but not limited to the requirements stated herein.

E. Requirements: Provide the following information complete, and in the manner described herein:

1. Hardware, Application Software, and Network Requirements: A system description including analysis and calculations used in sizing equipment required by the security systems. The description shall show how the equipment will operate as a system to meet the performance requirements of the systems. The following information shall be supplied as a minimum:
   a. Server(s) processor(s), disk space and memory size [expansion of existing]
   b. Workstation(s) processor(s), disk space and memory size

c. Description of site (field) control equipment (Controllers/Field Panels, Archivers, Modules) and their configuration
d. Operating System(s) Software, where software is provided or upgraded
e. Application Software, with Optional and Custom Software Modules supplied in this project
f. Integration Schemes: Proposed connectivity, software, development requirements, and SDK information, for inter-system communication.
g. Network bandwidth and reliability requirements
h. Number and location of LAN ports required
i. Other specific network requirements, preferences, and constraints
j. Backup/archive system size and configuration
k. Start-up operations
l. System power requirements and Uninterruptible Power Supply (UPS) sizing
m. Device/component environmental requirements (cooling and or heating parameters)

2. Shop Drawings: Shop Drawings shall be numbered consecutively and shall accurately and distinctly present the following information:
   a. Title Sheet
   b. Floor Plans: Showing devices, pull boxes, cabinets, conduits, and conductors in their proposed locations with device numbering scheme.
   c. Riser Diagram: Showing all conduit relationships between devices shown on the Floor Plans. Show all power sources.
   d. Single-Line/Block Diagrams: Show signal relationships of controls and devices within the system.
   e. Custom Assembly Diagrams: For each custom assembly such as Access Control Terminal Cabinets, receptacle assemblies, or door control panels, provide an assembly drawing illustrating the appearance of the assembled device. Include dimensions, assembly components, and functional attributes (momentary or alternate action switch, lens color, panel finish)
   f. Component Connection Diagrams
   g. For each equipment component such as a computer, video switcher, camera, or video recorder, show the rear elevation of the device and all connectors/terminations as a pictorial.
   h. Show the wire designations on connectors. Typical wiring detail where multiple of same device is provided.
   i. Show a schedule of the wire colors connected to the pins on each device connector.
   j. Equipment Wiring Diagrams
   k. Show a pictorial illustration of each equipment enclosure and/or terminal cabinet, including terminals, components, and wiring devices.
   l. Show the device nomenclature exactly as shown on the single line diagrams.
   m. Terminations: Show every termination and terminating cable, with applicable cable and wire numbers matching the single line diagrams.
      1) Every termination in the system must be documented.
      2) Termination information may be rendered as a wiring list(s), if properly coordinated with, and referenced to, typical component and single-line diagrams. Otherwise, the Shop Drawings shall show a pictorial of every component in the system, with its terminations.
   n. Show wire colors for each terminal.

o. For each wire exiting the enclosure, show the destination of the wire by floor, room number and the drawing number of the panel where the wire terminates.
p. Provide working dimensions and erection dimensions.
q. Arrangements and sectional views
r. Necessary details, including complete information for making connections between work under this Contract, existing work, and work under other Contracts.
s. Stock or standard drawings will not be accepted for review unless full identification and supplementary information is shown thereon in ink or typewritten form.
t. Duplicate of design drawings may be used where each sheet is modified to reflect contractor coordination, specific requirements of the project and multidiscipline conditions.
u. Each Drawing or page shall include:
v. Project name, Project Number, and descriptions.
w. Submittal date and space for revision dates.
x. Identification of equipment, product, or material.
y. Name of Contractor and Subcontractor.
z. Name of Supplier and Manufacturer.
aa. Relation to adjacent structure of material.
bb. Physical dimensions clearly identified.
cc. ASTM and Specifications references.
dd. Identification of deviations from the Contract Documents.
ee. Contractor's stamp, initialed or signed, dated, and certifying to review of submittal, certification of field measurements and compliance with Contract.
ff. Location at which the equipment or materials are to be installed. Location shall mean both physical location and location relative to other connected or attached material.

3. Equipment Submittals
   a. Provide a Title Page, with project name, the Security Integrator’s name and address, contact information, date of submission, and submission revision number.
   b. Provide a Parts List, for proposed equipment, materials, components, and devices, listing the following information for each line item:
   c. The system types
   d. Model numbers
   e. Specification sheet page reference
   f. Provide Manufacturers Specification Sheet with descriptive information for equipment, materials, components, and devices. Number each page, to correspond with the Parts List.
   g. Clearly delineate (with highlighter, arrow, or underline) on each specification sheet, specific model numbers, options and configurations being proposed for this project.
   h. Indicate kinds of materials and finishes for equipment where more than one option is presented.
4. Acceptance Testing Plan
   a. Submit a written document detailing the test procedures to be followed in evaluating and proving the installed system(s).
   b. Provide a sample of the test forms to be used for each system and for each component of each system.

c. Include all tests required by the equipment manufacturer and by this Specification.

5. Spare Parts List, include where requested by Owner
   a. Submit a list of recommended spare parts.
   b. Spare parts shall comprise a minimum of 5% or minimum of 2 each of field devices, device termination boards and a minimum of 1 system controller boards.
6. Training Program
   a. Submit a training program 10 working days prior to scheduled training to be followed in training key employees in the operation and maintenance of the installed system at the project site. The proposed training program shall be designed to provide a level of basic competence with the system for selected personnel. These selected personnel shall then be expected to train other personnel as required, utilizing the training that they have been given and the body of training documentation provided by the Security Integrator. This plan shall comply with the requirements stated in the "Training" section, of these Specifications, all stated hours of which shall be considered to be classroom hours.
   b. Submit a curriculum to account for, and relate, each subject to actual training time. All required hours shall be accounted for in this curriculum.
   c. The training plan shall cover the overall system, each individual system, each subsystem, and each component. The plan shall also cover procedures for database management, normal operations, and failure modes with response procedures for each failure. Each procedural item must be applied to each equipment level.

F. The Owner will return unchecked any submittal which does not contain complete data on the work and full information on related matters.

G. Verification: The contractor shall check and acknowledge all shop drawings and shall place their signature on all shop drawings submitted to the Owner. Security Integrator 's signature shall constitute a representation that all quantities, dimensions, field construction criteria, materials, catalog numbers, performance criteria and similar data have been verified and that, in their opinion, the submittal fully meets the requirements of the Contract Documents.

H. Timeliness: The Security Integrator shall schedule, prepare and submit a complete shop drawing assembly in accordance with a time-table that will allow their suppliers and manufacturers sufficient time to fabricate, manufacture, inspect test and deliver their respective products to the project site in a timely manner so as to not delay the complete performance of the work.

I. Departure from Contract Requirements: If shop drawings show departures from the Contract requirements, the Security Integrator shall make specific mention thereof in their letter of transmittal, otherwise review of such submittals shall not constitute review of the departure. Review of the drawings shall constitute review of the specific subject matter for which the drawings were submitted and not of any other structure, materials, equipment, or apparatus shown on the drawings.

J. Security Integrator Responsibility: The review of shop drawings will be general and shall not relieve the Security Integrator of responsibility for the accuracy of such drawings, nor for the proper fitting and construction of the work, nor for the furnishing of materials or work required by the Security Integrator. No construction called for by shop drawings shall be initiated until such drawings have been reviewed and approved.

K. Shop Drawing Submittal Review: The procedure in seeking review of the shop drawings shall be as follows:
   1. The Security Integrator shall submit four (4) complete sets of shop drawings with equipment submittals and other descriptive data with one copy of a letter of transmittal to the Owner for review thirty (30) working days after award of the contract. The letter of transmittal shall contain the project name, the Owner's Project Number, the name of the Security Integrator, the list of drawings submitted including numbers and titles, requests for any review of departures from the contract requirements and any other pertinent information. Drawings submitted for review shall be full-sized drawings, rolled and included with the equipment submittals.
   2. Drawings or descriptive data will be stamped "Reviewed", "Furnish as Corrected", "Revise and Resubmit", "Rejected" or 'Submit Specific Item' and one copy with a Letter of Transmittal will be transmitted to the Security Integrator with the return of submitted documents.
   3. If a shop drawing or data is stamped "Reviewed" or "Furnish as Corrected", no additional submittal is required for that shop drawing.
   4. If a shop drawing or data is stamped "Revise and Resubmit" or "Rejected", the Contractor shall make the necessary corrections and resubmit the documents as required above. The letter transmitting corrected documents shall indicate that the documents are re-submittals.
   5. If any corrections, other than those noted by the Owner, are made on a shop drawing prior to resubmittal, such changes should be pointed out by the Security Integrator upon resubmittal.
   6. The Security Integrator shall revise and resubmit the shop drawing as required, until they are stamped either "Reviewed" or "Furnish as Corrected."
   7. After the Security Integrator's submittal or resubmittal of shop drawings, the Owner shall be provided with fifteen (15) working days for review. Should the Owner require additional review time above and beyond the stated fifteen (15) working days, the Security Integrator may ask for a time extension and/or monetary compensation, if they can present valid, factual evidence that actual damages were incurred by the Security Integrator. The Owner shall determine the amount of the time extension and/or the monetary compensation to be awarded to the Security Integrator.
   8. The Owner will not issue a "Notice to Proceed" until shop drawings are reviewed, unless otherwise approved by the Owner.

L. The Contractor shall be responsible for extra costs incurred by the Owner caused by the Contractor's failure to comply with the procedure outline above.

1.15 OPERATING AND MAINTENANCE MANUALS: RECORD DOCUMENTS

A. Phase One: Notwithstanding requirements specified elsewhere, submit the following labeled as the "Operating and Maintenance Manual" within thirty (30) days after Final Acceptance of the Installation:
   1. Record Drawings: Submit two (2) copies of revised versions of drawings as submitted in the "Shop and Field" and "Equipment Wiring Diagrams" Submittals showing actual device locations, conduit routing, wiring and relationships as they were constructed. Include nomenclature showing as-built wire designations and colors. Drawings shall include room numbers coinciding with Owner space planning numbering. Drawings shall be submitted in electronic editable AutoCAD files, in ".dwg" format, on USB drive or DVD disks.
   2. Manuals: Submit two (2) copies of each of the following materials in bound manuals, or electronic PDF copies on USB drive or DVD discs, with labeled dividers:

a. A final Bill of Material for each system.
b. Equipment Instruction Manuals: Complete, project specific comprehensive instructions for the operation of devices and equipment provided as part of this work.
c. Manufacturers Instruction Manuals: Specification sheets, brochures, Operation Manuals, and service sheets published by the manufacturers of the components, devices and equipment provided.
d. Include information for testing, repair, troubleshooting, assembly, disassembly, and recommended maintenance intervals.
e. Provide a replacement parts list with current prices. Include list of recommended spare parts, tools, and instruments for testing and maintenance purpose.
f. Performance, Test and Adjustment Data: Comprehensive documentation of performance verification according to parameters specified herein.
g. Warranties: Provide an executed copy of the Warranty Agreement and copies of all manufacturers' Warranty Registration papers as described herein.

B. Phase Two: Within fourteen (14) days of receipt of engineer reviewed Operating and Maintenance Manual (Phase One), submit three (3) electronic copies in AutoCAD editable dwg format of the reviewed Record Drawings and three (3) copies of the reviewed Operating and Maintenance Manuals to the Owner, on USB drive or DVD disks.
1. The Security Integrator shall provide to the Owner one (1) copy of new executive and user software, including required graphical maps, on USB drive or DVD-ROM disks.
2. Sufficient information, (detailed schematics of subsystems, assemblies, and subassemblies to component level) clearly presented, shall be included to determine compliance with drawings and specifications.

1.16 CHANGES

A. Before proceeding with changes or claims for extras, the Security Integrator shall provide written notice, secure prior written approval from the Owner, and substantiate actual cost of each change or claim.

1.17 NOTIFICATION

A. The Security Integrator shall not shut off any existing systems. The Security Integrator shall give the Owner at least 14 calendar day notice of any requirement to shut off or interfere with existing alarm, access control, regulating, computer or other service systems. The Owner will arrange and execute any shutdown. Work such as splicing, where approved, and connections necessary to establish or re-establish any system shall be completed by the Security Integrator in close coordination with the Owner.

1.18 INTERFERENCE WITH THE FACILITY

A. Transportation and storage of materials at the facility, work involving the facility, and other matters affecting the habitual use by the Owner of its buildings, shall be conducted so as to cause the least possible interference's, and at times and in a manner acceptable to the Owner. The Security Integrator shall make every effort to deliver equipment per the schedule required by the project.

1.19 WARRANTY

A. Furnish and guarantee maintenance, repair and inspection service for the system using factory trained authorized representatives of the manufacturer of the equipment for a period of one year after final acceptance of the installation.
B. Third Party Device warranties are transferred from the manufacturer to the Security Integrator, which may then transfer third party warranties to the Owner. Specific third-party warranty details, terms and conditions, remedies, and

procedures, are either expressly stated on, or packaged with, or accompany such products. The warranty period may vary from product to product. These products include but are not limited to devices that are directly interconnected to the field hardware or computers and are purchased directly from the manufacturer. Examples may include but not be limited to, servers, cameras, video recorders, card readers, and computers.

C. Purpose
    1. The Security Integrator shall repair any system malfunction or installation deficiency discovered by the Owner or their representatives during the burn in and warranty period.
    2. The Security Integrator shall correct any installation deficiencies found against the contract drawings and specifications discovered by the Owner or their representatives during the warranty period.
D. The service contract shall cover equipment and software related to this contract, and shall provide for the following parts and services, without additional cost to the Owner:
    1. Quarterly Inspection, Preventative Maintenance and Testing of equipment and components
    2. Regular Service, Emergency Service, and Call-Back Service
    3. Labor and Repairs
    4. Equipment and Materials
E. Response Time: Response time for service calls.
    1. Emergency service calls where system is not responding to staff directed commands through the computer systems shall be within 2 hours to the project site.
    2. Emergency service calls where controllers are not reporting shall be within 2 hours to the project site.
    3. Normal service calls for device malfunctions shall be within 24 hours during normal working hours to the site.
F. Repair Time: The Security Integrator shall stock parts in sufficient quantities such that repair, or replacement shall be guaranteed within 12-hours. Temporary replacements within this time period shall be acceptable, provided temporary replacements do not compromise system functionality, and provided permanent replacement is achieved within 72 hours. [Security Integrator may contact owner representative for use of owner supplied spare parts where delay of system repair will have negative impact on system performance]
G. Commencement: The warranty begins at the time of issuance of the statement of "Final Acceptance of the Installation" by the Owner.
H. Transferability: The warranty shall be transferable to any person or persons at the discretion of the Owner.
I. Transmittal: A copy of this Warranty shall be delivered to and signed for by the Owner's representative whose primary responsibility is the operation and care of these systems. A copy of the signed Warranty document shall be delivered for review as part of the Final Submittals.
J. Registration: Register Warranty papers for all equipment and software in the name of the Owner. Furnish reproductions of all equipment Warranty papers to the Owner with the Final Submittals.
K. Sub-Contracting: Warranty service work may not be sub-contracted except with specific permission and approval by the Owner.
L. Resolution of Conflicts
    1. The Owner retains the right to resolve unsatisfactory warranty service performance at any time by declaring the work unsatisfactory, stating specific areas of dissatisfaction in writing.

2. If the Security Integrator or their approved subcontractor does not resolve such stated areas of dissatisfaction within thirty (30) days, the Owner may appoint any alternative service agency or person to fulfill the terms of the Warranty; the cost of which shall be borne by the Security Integrator. This action may be taken repeatedly until the Owner is satisfied that Warranty service performance is satisfactory. Satisfactory resolution of a malfunction shall be considered adequate when the device, equipment, system, or component which is chronically malfunctioning is brought into compliance with the standards of performance as contained herein and published by the manufacturers of the equipment installed.

1.20 PERMITS AND INSPECTIONS

A. Responsibility: Obtain permits and inspections required for the work. Permit and inspection costs will be borne by the Security Integrator.

B. Performance: Perform tests required herein, or as may be reasonably required to demonstrate conformance with the Specifications or with the requirements of any legal authority having jurisdiction.

C. Review: Obtain approvals from authorities responsible for enforcement of applicable codes and regulations to establish that the work follows all requirements of reference codes indicated herein and required by the appropriate jurisdiction. Make corrections, changes, or additions as required and deliver certificates of acceptance, operation, and/or compliance with the "Operating and Maintenance Manuals" as described herein.

1.21 TRAINING

A. On-Site Training

1. General: Present, review and describe equipment and materials to the Owner and Owner's operating personnel and fully demonstrate the operation and maintenance of the systems, equipment and devices specified herein.
2. Training shall comprise two separate levels of training
   a. User Group upon substantial completion of the project
      1) User group training shall include a site/building walk through indicating locations of equipment and their usage
      2) User group training shall include the operation of workstation capability of system monitoring, command override and report generation.
   b. Maintenance Group upon completion of the project prior to close out
      1) Maintenance group training shall include a site/building walk through indicating locations of equipment and their usage
      2) Review of as-build documentation at each controller location
      3) Trouble shooting techniques in hardware and software
3. The training shall cover the overall system, each individual system, each subsystem, and each component. The training shall also cover procedures for database management, normal operations, and failure modes with response procedures for each failure. Each procedural item must be applied to each equipment level.
4. Duration: Provide at least 2 hours of on-site training on each system for each group of designated representatives of the Owner at a location convenient to the Owner.
5. On-site training shall commence as follows:
   a. EACS: Just prior to completion of the first phase of work which establishes the new EACS control over entry and exit portals.
   b. VSS: Just prior to completion of the first phase of work which establishes the new VSS control over video cameras.

B. Include with new systems Software Tutorials: Contractor shall provide a professionally rendered, customized computer-based multimedia tutorial for training a user to use each security system application. Tutorials shall be provided on DVD/Portable USB media.
   1. Provide professional tutorial of each software screen option, with Owner approval of content. Tutorial shall include screenshots and dynamic recording of screen activity for each system function.
   2. Provide end user tutorial for Department of Public Safety approved monitoring, administrative, and response processes. Tutorial shall include screenshots and dynamic recording of screen activity for each system function.
   3. Provide Facilities Management approved tutorials of maintenance and troubleshooting processes. Tutorial shall include screenshots and dynamic recording of screen activity for each system function.

1.22 SAFEGUARDS AND PROTECTION

A. Barriers: Provide and maintain suitable barriers, guards, fences, and signs where necessary to accommodate the safety of others relative to and/or for the protection of this work.
B. Regulations: Comply with OSHA, Federal, State, and local regulations, and standards pursuant to this work.
C. Protection: Protect all materials and equipment to prevent the entry or adhesion of any and all foreign material. If necessary, cover equipment with temporary protective material suitable for this purpose.
D. Finishing: Check, clean and remove defects, scratches, fingerprints, and smudges if necessary, from all equipment and devices immediately prior to Acceptance of the Installation.
E. Damage: Replace all damaged or defective material or work at no additional cost prior to Final Acceptance.
F. Documentation: Provide written description of accidents by workers, students and staff of any incident occurring on the project. Report incident in writing to Owners representative immediately and to the Project Manager for follow up.

1.23 PRODUCT DELIVERY, STORAGE AND HANDLING

A. Delivery: Unless otherwise noted, pre-testing or configuration is required by the Security Integrator, deliver materials to the job site in manufacturer's original unopened containers, clearly labeled with the manufacturer's name and equipment model identification number.
B. Storage and Handling: Store and protect equipment in a manner which will preclude damage.

1.24 EQUIPMENT COMPATIBILITY REQUIREMENTS

A. While individual items of equipment may meet the equipment specifications and in fact meet the system specifications, the total system shall be designed so that the combination of equipment actually employed does not produce any undesirable effects such as signal distortion, noise, transients or crosstalk interference is when electrically associated with itself or other equipment.

1.25 OWNER'S RIGHT TO USE EQUIPMENT

A. The Owner reserves the right to use equipment, material and services provided as part of this work prior to Acceptance of the Work, without incurring additional charges and without commencement of the Warranty period.

PART 2 PRODUCTS

2.1 GENERAL

A. These general criteria shall apply to "Part 2-Products" of all Access Control specifications that are a part of this work.

B. Product Acceptability: Products sections contain lists of Owner acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified. Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether a submitted substitution is deemed to be "equivalent" to that specified.
C. Manufacturers Specification Reference: Where a specific material, devices equipment or systems are specified directly, the current manufacturers' specification for the same becomes a part of these specifications, as if completely elaborated herein.
D. Equipment shall be new and the current model of a standard product of a manufacturer of record. A manufacturer of record shall be defined as a company whose main occupation is the manufacture for sale of the items of equipment supplied.
E. For each item of equipment offered, manufacturer shall maintain:
    1. A factory production line.
    2. A stock of replacement parts.
    3. Engineering drawings, specifications, operating manuals, and maintenance manuals.
    4. Manufacturer shall have published and distributed descriptive literature and equipment specifications on each item of equipment offered.
F. Complete System: Auxiliary and incidental equipment necessary for the complete operation and protection of the systems specified herein shall be furnished and installed as if specified in full.
G. Similar Devices: Similar devices within a system shall be identical unless specific color variances are required by the Owner or Architect.
H. Safety: Unless otherwise specified, equipment shall be UL rated individually and listed as an assembly. Electronic equipment shall be of the dead front type, having no exposed live electrical connections, terminals or exposures to hands-on operating surfaces or other exposed surfaces during any power-on condition. Every live electrical connection, terminal or exposure shall be covered with durable, removable insulating material.
I. Rack Mounting: Rack-mounted electronic equipment shall be specifically designed or modified for standard 19-inch rack mounting unless otherwise noted.
J. Keying: Key panels identically where provided for similar usage within a system. Coordinate lock types with Owner.
K. Framing: Floor supported units shall be substantially framed and supported. All bolted connections shall be made with self-locking devices.
L. Aesthetics: Coordinate console or control panels so that their general appearance is similar. Provide locking panel covers on recessed, semi-recessed and surface mounted control panels not located in equipment rooms. Control panels shall be contained within or mounted to formed and welded aluminum or steel back-boxes. Operating panels shall be recessed within the back-box to a depth sufficient to permit a locking hinge panel cover to close completely without affecting any device within the enclosure.
M. No contractor proprietary equipment will be permitted without prior approval from the Owner.
N. Operational Voltage: Devices connected to the fuse or breaker protected electrical system and all auxiliary equipment necessary for the operation of the equipment associated with systems specified herein shall be designed to operate from 105 to 130 volt, 60 Hertz, alternating current service, with stable performance, fully in accordance with these specifications, and shall have integral fuse or circuit breaker protection.

O. Contractor-fabricated items shall be provided with fuses that indicate when they are blown or defective.
P. Protection devices shall be located to facilitate replacement, resetting or observation of status without demounting the associated unit and/or de-energizing adjacent equipment.
Q. Manufacturer's Recommendations: Components and devices shall be operated in accordance with recommendations of the manufacturer and shall contain sufficient permanent identification to facilitate replacement.
R. City of Los Angeles Testing Requirements
    1. Equipment, devices, and assemblies shall meet the City of Los Angeles' requirements for listing and labeling, which includes UL listing and labeling for manufactured equipment.
    2. UL Listing: For devices and assemblies with proper UL listing and labeling, stickers shall be accessible and visible to the Inspectors. Paperwork shall also be available during inspections and shall be provided to the Owner as part of the close out documentation.
    3. Unlisted Devices and Assemblies: Devices and assemblies without prior listing from testing authorities accepted by the City of Los Angeles, shall be tested by an agency acceptable to the City of Los Angeles prior to inspection, to obtain a listing and label. Documentation on the testing and approval shall be provided to the Owner as part of the close out documentation.

2.2 MISCELLANEOUS PRODUCTS

A. Cabinets: LifeSafety, Hoffman, Lenel or equal, assembled and wired with all components and as indicated on the drawings. Coordinate color, location, and trim with the Owner.
B. Cable Termination Devices: Screw-Type Barrier Blocks: Marathon/Kulka 601 or Kulka 601-3700 Series, TRW-Cinch, 140, 141 and 142 Series, Phoenix or Buchanan.
C. Relays: Control relays to be provided by the Security Integrator shall meet or exceed the following
    1. Provide U.L. listed single pole, double throw (SPDT) type, unless otherwise noted on the drawings, with silver tin oxide contacts.
    2. They shall have a contact rating of 250 V AC/DC at 6A on normally open contacts and 2A on normally closed contacts.
    3. Control relay bases shall be UL listed, DIN rail mounted style, and shall be compatible with the proposed control relay. They shall have screw terminals for all wiring leads accepting conductors up to size 14 AWG. Relay bases shall have provisions for accepting machine printed labels.
    4. Control Relays: Provide relays and bases by Potter & Brumfield, Square D, or equal.
    5. Power Relays: Provide American Electronic Components "Durakool" mercury wetted relays or equal by Potter & Brumfield.
D. Wire and Cable Management: Provide Thomas and Betts Ty-Duct Series of Slotted Wiring Ducts, or equal by Marathon, or Eaton. Wiring duct shall be used within cabinets, enclosures, and terminal boxes for the distribution and management of cables within the enclosures. Provide compatible mounting hardware, end caps, labeling and appurtenances to form a complete wire management system. Comply with manufacturers recommended maximum fill schedules.
E. Theft Proof Screws
    1. Provide Tamperproof security fasteners for the installation of security equipment, cabinets, enclosures and pull boxes in accessible locations. Provide Bryce Fastener PentaPlus series, TP3 style by Tamperproof Screw Company, or equal by Hudson Fastener.

2. Provide six (6) compatible screw drivers and transfer to the Owner prior to final acceptance testing.

F. Equipment Enclosure
   1. Indoor Wall Mount Rack Enclosures
      a. Provide Atlas WMA Series, or Bud Cabinets Emperor Series, or equal, sectional wall cabinets, with door and mounting rails for standard 19" rack mount equipment.
      b. Cabinet shall be in three sections: solid door, center section, and rear section. Door and center section shall swing out, permitting service from the rear without disassembling equipment. Center section depth shall be 15", minimum.
      c. The Security Integrator shall size the height of the cabinet to house applicable equipment, terminals, wire, and devices in a neat and workmanlike manner.
   2. Indoor Enclosures: Refer to Security Terminal Cabinet (STC) configurations within Specification Section 28 13 00 Electronic Access Control System
   3. Outdoor Enclosures: Provide Lifesafety or Hoffman DesignLine Type 3R or Type 4 Enclosure, or equivalent, with 10 Gage steel body and door, swing-out rack mount, and extension ring kits as required to house specified equipment. Provide tamper resistant key lock. The Security Integrator shall size the cabinet to house applicable equipment, terminals, wire, and devices in a neat and workmanlike manner.

2.3 ACCESS CONTROL RACK AND CONSOLE MATERIALS

A. Equipment Racks: The Security Integrator shall provide racks where shown on the plans. Racks shall be designed to house required equipment and shall also include the following elements.
   1. Top Fan Panel: Provide top panel with exhaust fans, safety guard, cord, and plug. Install a multi-fan top panel in each rack bay, with enough low-noise fans to provide the required cooling.
   2. Pullout Work Surface: 3 ½" x 20" rack mountable work surface.
   3. Sliding shelves for computers and keyboards.
   4. Provide blank plates to cover unused front spaces.
   5. Coordinate console color, trim and finish with the Owner.
   6. Provide leveling feet, floor mounting kit, earthquake kit, rack connector kit, keyed locking hardware and miscellaneous hardware to provide a sealed and finished appearance.
   7. Refer to drawings for further details.
   8. Obtain approval of color and finishes with Owner prior to delivery.
   9. Console/Rack shall be by Winsted, Middle Atlantic or Owner approved equal

2.4 TEST EQUIPMENT

A. The Security Integrator is responsible for providing test equipment required to test the system in accordance with the parameters specified. Unless otherwise stated, the test equipment shall not be considered part of the system and retain ownership of the equipment. The Security Integrator shall furnish test equipment of an accuracy better than the parameters to be tested.
B. The test equipment list shall be furnished as a part of the submittal.
C. Readiness: Keep test equipment at hand and maintain in calibrated condition at the jobsite as required for routine and performance testing of this work.

PART 3 EXECUTION

3.1 GENERAL

A. Perform this work in accordance with acknowledged industry and professional standards and practices, and the procedures specified herein.

B. Aesthetics are an important consideration in this installation. Components shall be installed to have aesthetically pleasing results per Owner and Architect requirements. Actual locations of visible components shall be coordinated in advance with Owner and Architect.
C. The Contractor shall insure that installation personnel understand the requirements of this Specification.

3.2 COORDINATION

A. General
   1. This Contract involves functioning systems. Coordination with the Owner is critical. Do not interrupt any functioning system without complying with the requirements of "Notification" section of this specification.
   2. Coordinate the work with the Owner and all trades to assure that where this work interfaces to other trades, those interfaces are provided, complete and functional.
   3. Meet with a representative of the Owner and each trade. Identify devices needed to complete functional operation of this work which are being provided by Owner, General Contractor, or another trade, and assure that the work being provided by others will be acceptable.
   4. Make sure work by others is scheduled in order that this work can be installed in a timely fashion.
   5. Verify dimensions, and work by others which may be necessary to facilitate the work and coordinate with other trades. Assure that related work by others is coordinated with this work.
   6. Verify field conditions. Regularly examine construction and the work of others which may affect the work to ensure proper conditions are provided for the equipment and devices before their manufacture, fabrication, or installation. Be responsible for the proper fitting of the systems, equipment, materials, and devices provided as part of this work.
B. Required Resources: Become familiar with the available access and space for equipment and any potential interference requiring coordination. Coordinate with the Owner to assure that adequate electrical and HVAC services are available. Provide the physical space for equipment, and ample access room for installation and maintenance of equipment.
C. Positioning Members: Provide additional support or positioning members as required for the proper installation and operation of equipment, materials and devices provided as part of this work as approved by the Owner without additional expense.
D. Interface Devices: Provide items necessary to complete this work in conformance with the Contract Documents or the satisfaction of the Owner without any additional expense.
E. Equipment shall be mounted with sufficient clearance to meet applicable codes and facilitate observation and testing. Securely hang and/or fasten with appropriate fittings to ensure positive grounding, free of ground loops, throughout the entire system. Units shall be installed parallel and square to building lines.
F. Installation shall comply with "Codes and Standards" section of this specification. Where more than one code or regulation is applicable, the more stringent shall apply.
G. Where new equipment is replacing old equipment, the Security Integrator is responsible for removing the old equipment and doing repair work necessary to meet standards determined by Owner.
H. Install fire stopping for penetrations in slabs and firewalls to meet code at the completion of work and prior to final testing demonstration to Owner.

I. Project Documentation: Review project documentation. If the Contractor perceives conflict or ambiguity in the contract documents, he shall seek interpretation from the Owner. Failure to do so may result in remedial work.

J. Project Schedule: Immediately obtain and follow the project schedule established by the Owner. Failure to maintain the schedule may result in a requirement by the Owner to expend extra effort until the project schedule has been achieved.

K. Schedule Changes: Time is of the essence of this agreement. In the event that it becomes necessary for the Contractor to expend "extra effort" to complete the work according to schedule changes not covered above, the Security Integrator agrees to cooperate with the Owner in good faith to complete the work according to schedule requirements.

L. Supervision: Maintain a competent supervisor and supporting technical personnel acceptable to the Owner during the entire installation. A change of supervisor during the project shall not be acceptable without prior written approval from the Owner.

M. Work and Manpower Rules: Comply with applicable jobsite work and manpower regulations.

N. Found Conflicts: Continuously make known to the Owner, conflicts discovered which may affect the orderly completion or the specified performance of this work. Cooperate with the Owner and other trades to accommodate such changes as may be necessary to resolve found conflicts.

O. Coordination Difficulties: Promptly notify the Owner in writing of any difficulties which may prevent proper coordination or timely completion of this work. Failure to do so shall constitute acceptance of construction as suitable, to receive this work, except for defects that may develop in the work of others after its execution.

P. Environmental: Verify the intended location(s) for equipment is suitable for the equipment. If conditions such as temperature, humidity, dust level or the like require modification, make it known to the Owner immediately upon award of the contract. If equipment requires strict environmental conditions (dust limitations, etc.), notify the Owner immediately upon award of the Contract. Failure to notify the Owner of such conditions shall constitute acceptance of the conditions and any later required modifications to the equipment or the environment shall be at the sole cost of the Security Integrator.

Q. Extra Effort: The Owner retains the right to require the Security Integrator to expend whatever extra effort as may be required, in event the Security Integrator fails to perform satisfactorily at any milestone date, unless such delay is approved in writing by the Owner, or it can be proved by the Contractor that such delay was caused by other contractors, or Owner's intransigence relating to Owner requested changes in the scope of work. Any costs pursuant to such extra effort will be borne solely by the Contractor. If Project Schedule delays are approved, provide the Owner with monthly revisions of the Project Schedule reflecting actual performance vs. the schedule.

3.3 SEISMIC PROTECTION

A. General

1. Seismic protection criteria: Electrical and mechanical machinery installations in any Seismic Risk Zone of the Uniform Building Code Seismic Risk Map shall be protected from earthquakes.
2. Protection criteria for these zones shall be a Horizontal force Factor not less than required by code or agency, considered passing through the machinery center of gravity in any horizontal direction.
3. Unless vibration isolation is required to protect machinery against unacceptable structure transmitted noise and/or vibration, machinery shall be protected from earthquakes by rigid structurally sound attachment to the

load supporting structure. The number shall be determined by calculations performed by a registered California professional engineer, as verified by the seismic restraint vendor.

4. Use protected spring isolators, or separate seismic restraints, to protect vibration isolation machinery.
5. Seismic snubbers and protected spring isolators shall be seismic protection-rated along three principal axes, proven by independent laboratory testing or analysis, by an independent, licensed structural engineer.

B. The Contractor shall be responsible for the design of their method for seismic restraint systems and shall supply all seismic calculations and details to the Owner for review. The Contractor shall supply to the Owner's Representative details of the forces exerted by their restraints, anchorages, and other points of attachment.

C. Electrical and mechanical equipment shall be installed in accordance with the following guidelines:

1. SMACNA Publication: Guidelines for Seismic Restraints of Mechanical Systems
2. California Code of Regulations (CCR), Title 24, Division 22.
3. NUSIG – National Uniform Seismic Installation Guidelines

D. Contractor shall submit shop drawings for the mounting of equipment, fixtures, cabinets, consoles, conduit, and cable support racks. [where required] These drawings shall be prepared, stamped, and signed by a Registered California Structural Engineer.

3.4 WORKMANSHIP

A. The installation shall be performed in a professional and workmanlike manner.

B. On a daily basis, clean up and deposit in appropriate containers debris from work performed under the appropriate Specification sections. Stack and organize parts, tools and equipment when not being used.

C. Preparation, handling, and installation shall be in accordance with the Manufacturer's written instructions and technical data appropriate to the product specified.

D. Work shall conform to the National Electrical Contractors Association "Standard of Installation" for general installation practice.

E. At the conclusion of the installation, work areas, including panel boxes, shall be vacuumed, and cleaned to remove debris and grease.

3.5 EQUIPMENT ENCLOSURES, RACK AND CONSOLE INSTALLATION

A. Construction: Coordinate access openings and wire paths through the cabinets for all desk mounted devices.

B. Compliance: Comply with powering, conduit entry and grounding practices as described herein and as required by code.

C. Coordination of Access: Coordinate the installation of access covers, hinged panels, or pull-out drawers to ensure complete access to terminals and interior components. Access shall be designed such that demounting or de-energizing of equipment is not required to gain access to any equipment.

D. Enclosures: Fasten removable covers containing any wired component with a continuous hinge along one side with associated wiring secured and dressed to provide an adequate service loop. Appropriate stop locks shall be provided to hold all hinged panels and drawers in a serviceable position.

E. Service Loop: Provide a wiring service loop allowing relocation of termination to any point within the enclosure.

3.6 CUTTING, PAINTING AND PATCHING

A. Structural members shall not be drilled, bored, or notched in such a manner that shall impair their structural value. Cutting of holes in structural members, if required, shall be done with core drills and only with the specific approval of the Owner for each instance. Provide means to identify rebar in slabs prior to drilling.

B. Walls and other architectural features that require cutting or repair during the installation process shall be returned to their original condition, including the matching of colors and finishes to the satisfaction of Owner, and at no additional cost to Owner.

3.7 GROUNDING PROCEDURES

A. Provide grounding of systems and equipment in accordance with manufacturer's recommendations, local electrical codes, and industry standards.
B. Signal Ground: Signal ground shall be derived from the one main electrical panel which serves all equipment herein.
C. Grounding procedures for wire, equipment and devices shall be in strict accordance with manufacturers' recommendations and standard installation practices.
D. Equipment enclosures of an assembly shall be grounded to the single grounding terminal strip of each assembly.
E. Multiple Powered System Isolation: Where powered devices of the same system exist in two or more locations and a different signal ground exists in each location, the system's communication signal shall be isolated from signal ground at both source and destination ends via modem, fiber optics or other equivalent method.
F. Contractor shall eliminate or correct potential ground-loop problems in a manner approved by the Engineer.
G. Shielding: Shielded cables of this section shall be grounded exclusively to Signal Ground. No shields shall be permitted to carry live currents of any kind. Shields shall be tied to Signal Ground at the signal source end only, unless otherwise noted or required by the manufacturer.

3.8 CONDUIT AND WIRE INSTALLATION PRACTICES

A. Conduit
    1. Conduit shall be 3/4 inch minimum unless noted otherwise on the drawings.
    2. Wires shall be installed in conduit or in another Owner approved raceway under the following conditions:
        a. Power cables.
        b. Exposed wiring.
        c. Wiring in areas where mechanical or environmental conditions may damage unprotected conductors; and,
        d. Where otherwise specified herein or required by code.
    3. Conduit or raceway that is not hidden must have its location and appearance be specifically approved by Owner. If approved, exposed conduit or raceway shall be run in such a fashion as to make it as inconspicuous as possible. Runs should follow existing building lines and should be square wherever possible.
    4. Verify conduit has been installed, de-burred and properly joined, routed, and terminated prior to pulling of cables.
    5. Apply a chemically inert conduit lubricant to wire and cable prior to pulling. Do not subject wire and cable to tension greater than recommended by the manufacturer.
    6. Secure wire and cable runs vertically in conduit for continuous distances greater than thirty (30) feet at the vertical run terminations. Non-coaxial cables shall be secured by screw-flange nylon cable ties or similar devices. Symmetrical clamping devices with split, circular or other wire conforming, non-metallic bushings shall be provided for other cables.
B. Wiring Without Conduit
    1. Wiring may be run in concealed spaces without conduit, in electrical trays (approved by Owner), and where otherwise shown on drawings, provided conductors are reasonably protected from mechanical and environmental damage.

2. Conductors run without conduit shall be approved, UL Listed, rated, and labeled for Plenum use.
3. Secure wire and cable with approved supports in accordance with the referenced standards and the Authority Having Jurisdiction.
4. Provide cable supports at a minimum of 4-foot intervals.
5. Equipment and devices shall be installed on approved electrical back-boxes. Do not install equipment and devices directly on walls, ceilings, or structural components without back-boxes.
6. Secure cables to cabinets, junction boxes, pull boxes and outlet boxes with approved cable clamps.
7. Independently support cables. Do not use other supports i.e., (suspended ceilings, suspended ceiling supporting members, lighting fixtures, mechanical piping, or mechanical ducts).
8. Support cable independently of junction boxes, pull boxes, fixtures, suspended ceiling T-bars, angle supports, and similar items.
9. Support cable using cable trays, D-brackets, support straps, support wires or other approved cable supports.
10. Fasten cable supports to building structure and surfaces.
11. In shared electrical trays, open ducts, and other cable runs without conduit, separate and strap Access Control cable so that it is clearly distinguishable from all other cables.
12. Clearly mark security system cables at minimum intervals of every 10-feet. Marking shall be with a permanent, printed label, color-coded tag, or other distinguishing marking. Felt tip pen marking on the cable is not acceptable.

C. New Wiring
1. After installation, and before termination, wiring shall be checked and tested to insure there are no grounds, opens, or shorts on any conductors or shields. In addition, wiring between buildings or underground and all coax cables shall have insulation tested with a megohmmeter and a reading of greater than 20 megohms shall be required to successfully complete the test.
2. Run wires continuously from termination to termination without splices. Splices at junction box locations may be allowed at the discretion of the Owner. Recommendations for splices at these points shall be established with Owner. Contractor shall obtain approval from the Owner before proceeding with splices.
3. If splices are required and approved by Owner, the wire shall be joined with solder, then heat-shrink tubed, taped, or otherwise protected in an approved manner to provide mechanical and electrical integrity. Wire nuts and/or electrical tape connections shall not be acceptable. Final connections shall be made at terminal boards with full tagging, labeling and documentation.
4. Water-resistant protection shall be continuous throughout the cable in parking areas, surface conduit, poles, in-slab pull-boxes, in-slab conduit, and underground conduit and pull-boxes, and in any areas subject to moisture and/or water infiltration.
    a. Splices/Junctions: Provide water-proof protection of splices and junctions, in surface conduit and boxes, in-slab conduit and pull-boxes, underground conduit, and underground pull-boxes, to prevent the entry of moisture or water into cables, splices or connections.
    b. Cable Entries: Provide water-blocking sealants at all conduit entries into pull boxes, junction boxes, back-boxes, cabinets, etc., to prevent the entry of moisture or water into the conduit and cable system.

D. Boxes: Provide a box loop for wire and cable routed through pull boxes or controller panels. Cable loops and bends shall not be at a radius less than that

recommended by the manufacturer. Coordinate pull box size with the Division 26 Contractor as necessary to accommodate this requirement.

E. Wire Lacing and Dressing: Dress, lace, tie or harness wire and cable vertically, horizontally and at right angles to the enclosure surfaces to prevent mechanical stress on electrical connections as required herein and in accordance with accepted professional practice. No wire or cable shall be supported by a connection point.

F. Non-Coaxial Connections: Make non-coaxial connections and approved splices within terminal cabinets (except microphone or line level) to screw-type barrier blocks with insulated crimp-type spade lugs. Size all lugs properly to assure high electrical integrity. Connect only one (1) wire per spade lug and not more than two (2) lugs per screw terminal.

G. Non-Coaxial splicing at device locations to equipment with wire leads shall be made with pre-approved wire Dolphin Connectors.

H. Shielded Cables: Shielded cables shall be insulated. Do not permit shields to contact conduit, raceway, boxes, terminal cabinets, or equipment enclosures. Tin terminated shield drain wires and insulate with heat shrinkable tubing.

I. Coaxial Splices: Coaxial splices, if required and approved, shall be on plate mounted dual barrel type insulated BNC connectors, secured in such a manner that no stress is placed upon the connector.

J. Unacceptable Conditions: Correct any unacceptable wiring conditions immediately upon discovery, and upon receiving notice to correct.

3.9 DATABASE PREPARATION, CHECKING AND ACTIVATION

A. Security Integrator to request Owner provided forms with completed nomenclature for each identified device no less than 30 days prior to programming. It is essential that the above activities be clearly identified on the Project Schedule, so database preparation is accomplished in sufficient time to permit orderly and on time system activation

B. It shall be the responsibility of the Owner to ensure the accuracy of the database information entered on forms by thoroughly checking completed data entry forms.

C. It shall be the responsibility of the Security Integrator to ensure that database formatting is correct prior to entry into the system and system activation.

D. Programming

1. The Security Integrator shall be responsible for the initial database entry for devices and equipment installed in this project into the existing system prior to activation. Location of program database entry to be confirmed with the Owner. The database shall consist of hardware and function-related information, i.e., system configuration, doors, alarm points, software parameters for system management, graphical maps, intercom interfaces, alarm information – access levels, automatic opening and locking schedules. A printout of the final database shall be provided to the Owner for review and approval prior to system activation.
2. Programming rights shall be provided by Career and Protective Services (CAPS) and the Department of Public Safety (DPS). Security Integrator shall coordinate with these services prior to the completion of installation to set a schedule for access to programming resources.
3. Follow all procedures and protocols for programming the system, in accordance with CAPS/DPS instructions.

E. System activation shall be the responsibility of the Security Integrator. Once the system and database have been demonstrated to be functioning properly according to manufacturer's guidelines and the system design, further database entries and upgrades shall be the responsibility of Owner, unless otherwise noted.

3.10 SOFTWARE UPGRADES

A. If more recent versions of the operating system or application software are made available to or requested by the Owner prior to system acceptance, these updated versions shall be installed and verified by the Security Integrator.
B. Before installing upgrade software, the Security Integrator shall ensure that existing database information is properly "backed-up" prior to any installation action.

3.11 START-UP RESPONSIBILITY

A. The Security Integrator shall initiate System Operation. Competent start-up personnel shall be provided by the Security Integrator on each consecutive working day until the System is functional and ready to start the acceptance test phase. If in Owner's judgment the Security Integrator is not demonstrating progress in solving any technical problems, the Security Integrator shall supply Manufacturer's factory technical representation and diagnostic equipment at no cost to Owner, until resolution of those defined problems. Where appropriate, the Security Integrator will bring the System on-line in its basic state (i.e., alarm reporting, facility code access control, etc.).
B. Properly ground each piece of electronic equipment prior to applying power.
C. Properly ground all shielded wire shields to the appropriate earth ground at the hub end only, not at the remote or device end.
D. Use a start-up sequence that incrementally brings each portion of the system on-line in a logical order that incorporates checking individual elements before proceeding to subsequent elements until the entire system is operational.

3.12 PRELIMINARY, Inspection, Acceptance Testing, and Commissioning

A. Provide Preliminary Testing, Inspection, Acceptance Testing, Burn-In and Commissioning Performance services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

3.13 FINAL PROCEDURES

A. Portable Equipment: Furnish portable equipment specified herein to the Owner, along with complete documentation for the materials furnished. Portable equipment shall be presented in the original manufacturer's packing, complete with manufacturer's instructions, manuals, and documents. Testing of portable equipment shall have been previously conducted by the Security Integrator.
B. Post Acceptance Work: Check, inspect and adjust systems, equipment, devices, and components specified, programming updates, at the Owner's convenience, approximately sixty (60) days after Acceptance of the Installation.

3.14 NOTICE OF COMPLETION

A. When the performance and acceptance requirements described above, including the Final Acceptance Test, have been satisfactorily completed, the Owner shall issue a Letter of Completion to Contractor indicating the date of such completion. The Notice of Completion shall be recorded by Contractor upon receipt of the Owner completion letter. This date of record shall be the start of the warranty period.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 05 53
IDENTIFICATION FOR ELECTRONIC SAFETY AND SECURITY

PART 1 GENERAL

1.1 DESCRIPTION

A. This specification section covers the furnishing and installation of nameplates, labels, wire markers, and other identification components for security systems.

B. Security Integrator shall furnish and install identification devices as specified on cables, cabinets, racks, and equipment.

1.2 PRECEDENCE

A. Obtain, read and comply with General Conditions and applicable sub-sections of the contract specifications. Where a discrepancy may exist between any applicable subsection and directions as contained herein, this section shall govern.

1.3 GENERAL CONDITIONS

A. In accordance with Section 28 05 00, Security System General Requirements

1.4 RELATED WORK

A. In accordance with Section 28 05 00, Security System General Requirements

B. In accordance with Section 28 08 00, Security System Testing and Commissioning

C. In accordance with Section 09 90 00, Paints and Coatings

1.5 SHOP DRAWINGS & EQUIPMENT SUBMITTALS

A. In accordance with Section 28 05 00, Security System General Requirements

B. Product Data:

1. Submit manufacturer's catalog literature for each product required.
2. Submit identification schedule including list of wording, symbols, letter size, color coding, tag number, location, and function.

1.6 WARRANTY

A. In accordance with Section 28 05 00, Security System General Requirements

1.7 REQUIREMENTS FOR IDENTIFICATION AND TAGGING

A. Cables, wires, wiring forms, terminal blocks and terminals shall be identified by labels, tags or other permanent markings. The markings shall clearly indicate the function, source, or destination of all cabling, wiring and terminals. The wire marking format contained in the shop drawings shall be utilized for conductors installed under this Specification. Cables and wires shall be identified, utilizing heat-shrink, machine-printed, polyolefin wire markers. Handwritten tags or marker on wiring are not acceptable.

B. Should a situation arise where the wire tagging format as shown on the shop drawings cannot be used, a substitute format shall be submitted which complies with the intent to provide documentation that will permit end-to-end tracing of all System wiring.

C. Terminal points shall be appropriately identified and labeled as shown on shop drawings.

D. Nameplates – General:

1. Provide laminated, engraved plastic nameplates with ½ -inch minimum high letters for all panels, enclosures and cabinets. Attach nameplates to enclosure with double-sided adhesive tape .
2. Include nameplate schedule on shop drawing submittals.
3. Install nameplates behind panel door in public areas and on panel face in equipment rooms.
4. Nameplate Color Schedule:
   a. Fed from Normal Building Power: Black letter on White label
   b. Fed from Emergency/ Generator Power: White letters on Red label

E. Panels shall be provided with permanently attached engraved lamicoid labels, as described in Item E, with identifying names and functions. Labels shall be consistent in form, color, and typeface throughout the system and must contain the name of the system or subsystem as part of the label textual information. Handwritten tags or marker type identification are not acceptable.

F. Equipment/Equipment Racks: Provide an engraved lamacoid label, as described in Item E, on the front of equipment including its designation as assigned and referenced consistently throughout this project.

G. Enclosures and Cabinets:
   1. Provide an engraved lamacoid label, as described in Item E, on the front of wall mounted ACP, IAP, and Power Supply enclosures and equipment racks including its designation as assigned and referenced consistently throughout this project.
   2. Place documentation within each equipment enclosure and/or terminal cabinet, the Security Integrator shall place a Single Line drawing of the system(s) and the respective Equipment/Terminal Cabinet Wiring Diagram in a clear plastic 8" x 11" sleeve permanently attached to the inside cover of the terminal cabinet. Drawings shall include cable and equipment label designations to match the labeling within the cabinet.
   3. In each equipment enclosure the Security Integrator shall place an as-built drawing depicting device locations served by the equipment within the enclosure, with identification that is identical to the wiring tags and with the software description of each point.
   4. In each equipment enclosure the Security Integrator shall place a copy of the USC Lenel System Excel Spreadsheet or equal document depicting device names, MAC addresses and IP addresses as indicated in the Lenel system.

H. Door Openings: For all doors controlled by the Lenel system, provide a P-touch label with the door name (as named in the Lenel program) on the top of the door edge on the hinge side. P-touch label shall be black lettering on white ¼" tape. Coordinate with Owner for exact location.

I. Lenel Panel Relays: All relays on Lenel panel boards shall be labeled with P-touch label ¼" tape, black lettering on a white label, identifying the USC door number associated with the relay. Architectural door numbers are not acceptable for these labels.

J. Panic Bar: All panic bars shall be labeled on the inside of the hardware with P-touch label ¼" tape, black lettering on a white label, identifying the location of the power supply feeding the door including room name and room number.

K. Wire and Cable: Identify wire and cable clearly with permanent labels wrapped around the full circumference within one-inch of each connection. Correlate the number designated on the associated Shop or Field Drawings. Assign wire or cable designations consistently throughout a given system. Each wire or cable shall carry the same labeled designation over its entire run, regardless of intermediate terminations.

L. Wireless Locking Systems
   1. PIMs shall be labeled on the front cover with the following information:
      a. PIM Unique ID (found with HHD under properties)
      b. Linked Door numbers and corresponding PIM channel/RS485 address (As well as Lenel corresponding identifier if different)
   2. Map of all PIM and AD400 locations shall be provided to the Owner as part of closeout documents with table identifying which locks are linked with which PIMs

PART 2 PRODUCTS

2.1 GENERAL

A. Product Acceptability: The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified and compatible with the existing USC system. Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified. Contractor may not use contractor proprietary interface modules for connections between field devices and controller.

B. Labeling:
   1. Provide intelligible permanent engraved identification function on or adjacent to panel assemblies, power supplies, and cabinets.
   2. Provide intelligible permanent label-maker labels for relays, controls, fuses and/or circuit breakers, patching jacks, connectors, receptacles, terminal blocks, indicators, switches, monitors, and servers.
   3. Labels shall be machine-printed. Hand-lettered labels shall not be acceptable.

C. Engraving, labels, decals or other identification on any device, equipment or miscellaneous component shall be coordinated with the associated Field and Shop and Equipment Wiring Drawings.

D. No proprietary identification on assemblies will be permitted other than the original manufacturer's labels and identification.

2.2 MISCELLANEOUS PRODUCTS

A. Wire and Cable Labels: Provide Brady Type B-321, dot matrix and thermal transfer printable sleeves, with permanent ink ribbon printing, or Thomas and Betts EZ-W/YHS, or equal. Sleeves shall be constructed of heat shrinkable, high density polyolefin film coated and shall have an ink-receptive top-coating. Labels shall be pre-printed to match the designations shown on the shop drawings, fitted to cables in the field, and heat-shrunk to secure their position. Labels should be placed such that they are easily accessed and readable after the device or panel is fully dressed.

B. Equipment Labeling: Unless otherwise noted herein, provide laminated three-layer plastic with engraved black letters on white background color. Minimum plastic thickness shall be 1/8". Letter size shall be 1/2" minimum for equipment and controls.

C. Cabinet/Enclosure Labeling: Unless otherwise noted herein, provide laminated three-layer plastic with engraved black letters on white background color. Minimum thickness shall be 1/8". Letter size shall be 1/2" minimum.

PART 3 EXECUTION

3.1 GENERAL

A. In accordance with Section 28 05 00, Security System General Requirements.

3.2 LABEL AND NAMEPLATE INSTALLATION PRACTICES

A. Degrease and clean surfaces to receive adhesive for identification materials.

B. Install labels and nameplates only when ambient temperature and humidity conditions for adhesive are within range recommended by manufacturer.

C. Install identifying labeling after completion of system installation.

D. Nameplate Installation:
   1. Install nameplate parallel to equipment lines.
   2. Install nameplate for each control equipment enclosure with high-quality double-sided adhesive tape.
   3. Install nameplates for each control panel and major control components located outside of the panel with high-quality double-sided adhesive tape.

E. Wire Marker Installation
   1. Install wire marker for each conductor at each connection.
   2. Mark data cabling at each end. Install additional marking at accessible locations along the cable run.

3. Install labels at data outlets identifying patch panel and port.

3.3 PRELIMINARY INSPECTION AND TESTING

A. Provide preliminary inspection and testing services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

3.4 FINAL PROCEDURES

A. Perform final procedures in accordance with section 28 05 00, Security System General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 07 00
SECURITY SYSTEM INTEGRATION

PART 1 GENERAL

1.1 DESCRIPTION

A. General Description: This specification section covers the provision of mechanisms which will support the exchange and recognition of information and commands between various Access Control systems at the [Indicate Site and Building] project.

B. Contractor shall coordinate with providers of systems listed herein to provide equipment, software, and configuration that will support the required functionality and performance.

1.2 QUALIFICATIONS

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

1.3 GENERAL CONDITIONS

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

1.4 RELATED WORK

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

1.5 SHOP DRAWINGS & EQUIPMENT SUBMITTAL

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

B. In addition to the requirements of Section 28 05 00, provide the following information for each system to be integrated:

1. Describe the integration architecture between systems. Provide a single-line diagram showing relationships between integrated components.
2. If a central integration processing component or user-interface (server, application) is proposed, describe the hardware and application software proposed.
3. A detailed description of how the interface will be accomplished between each system, including proposed connectivity, hardware, software, language, protocols, procedures, and standards.
4. Proposed Software Development Kit (SDK) and Version, where an SDK already exists from the component manufacturer. Provide development and capabilities information on the SDK and its proposed use on this project.
5. Development specification for custom software development, where the interface must be created specifically for the project.
6. A detailed list, or matrix, of information, commands, and other elements of the interface, delineating exactly what functions will be supported between each system, and how they will work.

1.6 OPERATIONS AND MAINTENANCE MANUALS

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.7 WARRANTY

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.8 SERVICE AND MAINTENANCE

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.9 TRAINING

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.10 EQUIPMENT COMPATIBILITY REQUIREMENTS

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.11 OWNER'S RIGHT TO USE EQUIPMENT

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

1.12 TECHNICAL REQUIREMENTS - ACCESS CONTROL SYSTEM INTEGRATION

A. General
   1. The Security Integrator shall be responsible for providing hardware and software interfaces to achieve the specified system performance described herein and, by reference, realize absolute and seamless compatibility with the related component systems.
   2. The Security Integrator shall ensure system additions and modifications provided under this scope of work have no negative effect on the individual components and systems, and their core functionality, and no permanent effect beyond that specified or implied by the scope of work.

B. Purpose
   1. Integration is the process of designing, deploying, and configuring independently operating systems with the ability to request, receive, extract, process, and act upon information from other systems.
   2. Successful system integration must address three fundamental issues:
      a. Functionality: What information is needed, how it is to be requested and processed, and what functions or activities need to occur upon receipt of the information.
      b. Connectivity: How systems will be connected together to support the communication of information and commands. (Special interfaces, wiring, networks, databases.)
      c. Communication: How information will be communicated between systems. (Instruction sets, language, protocols, formats, priority.)

C. Environment
   1. Integration components shall generally comprise special elements of independent subsystems, and shall be located within, or in close proximity to, the processing components of each independent subsystem. Where subsystems require special hardware or communications interfaces to support integration, the special hardware should be located near the independent subsystem processing components or network appliance, based on the manufacturers' recommendation. See the drawings for details on mounting locations.
   2. Central Administrative Post: Components of the main integration system operating shell may be distributed throughout the site/facility, in relation to the other integrated subsystems. The main EACS system monitoring is located in CAPS/PSA Central Command Center. System programming, rules configuration and control shall occur at a location designated by the Owner.
   3. Infrastructure and Connectivity
      a. Devices/Appliances: Appliances and devices shall be connected to their respective systems via the applicable communications network.
      b. System LAN/WAN Connectivity: System Servers and microprocessor-based Control Panels, shall reside on the Local Area Network (LAN) or Wide Area Network (WAN) tier designated for integrated components.

c. Enterprise: LAN networks will be connected to the University's Wide Area Network, to establish connectivity between sites and the PSA Command Center.

D. Attributes
1. The attributes of the integrated environment are primarily defined by the subsystems that are to be integrated. Verify existing system components to be expanded by this project.
2. Integrated systems comprise the processors, software, electrical control panels, data gathering panels, special data interfaces, and converters required to allow systems to communicate with each other, process information, and allow users to program and perform operations.
3. The following systems will be a part of the integrated environment:
   a. Electronic Access Control System (EACS)
   b. Video Surveillance System (VSS)
   c. Electronic Intrusion Detection System (EIDS)

E. Functions
1. The system shall provide the following automated processing rules, at a minimum:
   a. The object of "Access Control system integration" is to automatically configure the system to display, record, and report appropriate system activity to various elements of the system. Automatic configuration can free operators from difficult control tasks, give the operator more time to respond to events, reduce operator error, and ensure critical system tasks occur consistently.
   b. Access Control system elements (EACS/VSS) shall be electronically integrated in such a way as to enable video, video detection, database records and/or event-initiated instructions to be communicated between system components, to initiate recording, display, communication, and control activities.
   c. Event-Initiated Interface, General:
      1) The system shall support the capability to send and receive alarm and control messages between the EACS and VSS systems via a LAN communications link, using API, XML, or other industry-standard communication languages and formats, and shall act upon those messages received.
      2) Where integration may require the implementation of RS-232 interfaces, Security Integrator shall propose such integration to the Owner for approval, before proceeding with the work.
      3) Software routines required to accomplish the required data-interface with external equipment and controls will be fully developed, installed, tested and supported by the Security Integrator.
      4) The manufacturer of each applicable system will also support the data interface, and will be engaged by the Security Integrator to provide on-site technical assistance where required to prepare, repair, configure, and test the system to operational condition.
      5) Communication of event information between systems shall take place automatically and immediately, when the event is sensed by the system.
      6) "Hard-wired" interfaces used to support interactive video surveillance cameras, intelligent video, threat-based control, and other event-initiated functions shall not be acceptable, except as otherwise noted herein or shown on the design drawings.

d. VSS Event-Initiated Control
    1) Upon receiving event/alarm information from the EACS, the VSS system shall transmit camera pre-positioning commands to applicable pan/tilt/zoom cameras, and shall cause the system to process, display, and record applicable cameras.
    2) The system shall automatically position and focus one or more cameras, or sequence of cameras, on nearby alarm locations. Coordinate with the Owner on initial and alarm preset camera views and programming.
    3) Configure systems to automatically send camera positioning and display commands from the EACS systems to the VSS Virtual Switching and Recording Software, based upon EACS event data. The system shall:
        a) Automatically select, position, and focus one or more cameras on areas of concern;
        b) Automatically re-configure recording for the selected cameras, to record them in an enhanced format, at the highest available resolution, frame rate, and quality (all other cameras remain at their pre-programmed format);
        c) Automatically display the selected cameras on one or more monitors, client workstations, and other display devices, in a pre-selected configuration (single or multi-camera views).
e. This interface shall be implemented using the integration scheme described herein.
f. Recorder/Camera Control: Configure the EACS to allow control of the VSS system. At a minimum, the EACS should support the following VSS system functionality:
    1) Link alarms or events to a camera, with programmable pre-and post-alarm recording sequences.
    2) Fast-forward, rewind, pause, and print, pre-recorded video.
    3) View recorded video “tagged” or associated with EACS alarms or events.
    4) Access a Windows-style Tree view of connected cameras.
    5) Select camera icon from map to view live video.
    6) View a single live video feed in full-screen.
    7) View up to 4 simultaneous camera views in quad-view format.
    8) Receive and display digital video recorder generated alarms such as video loss and motion detection.
    9) Trigger conditional commands on digital video recorder generated alarms.
    10) Send video matrix commands via selected camera icon.
    11) View recorded video from History Activity report, and/or Alarm Monitor window.
    12) Identify alarms and events that have associated video available for review.
    13) Full video playback available at all EACS clients.
    14) View associated video from the Alarm Monitor window, based on reported alarms.
    15) Provide both manual and preset pan-tilt-zoom control.

PART 2 PRODUCTS

A. Not used. Refer to individual equipment sections for specified systems.

PART 3 EXECUTION

3.1 GENERAL

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

3.2 COORDINATION

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

3.3 WORKMANSHIP

A. Provide the work in accordance with Section 28 05 00, Access Control General Requirements.

3.4 EQUIPMENT, RACK AND CONSOLE INSTALLATION

A. Provide equipment, rack, and console installation in accordance with Section 28 05 00, Access Control General Requirements.

3.5 GROUNDING PROCEDURES

A. Provide grounding of all systems and equipment in accordance with Section 28 05 00, Access Control General Requirements.

3.6 CONDUIT AND WIRE INSTALLATION PRACTICES

A. Provide conduit, wire and cable installation in accordance with Section 28 05 00, Access Control General Requirements.

3.7 IDENTIFICATION AND TAGGING

A. Provide identification of wire, panels, and devices in accordance with Section 28 05 00, Access Control General Requirements.

3.8 DATABASE PREPARATION, CHECKING, AND ACTIVATION

A. Provide database preparation, checking and activation for systems and equipment in accordance with Access Control General Requirements, Section 28 05 00.

B. Security Integrator shall coordinate with the Owner to determine the required pre-programmed surveillance, rule-setting, and event-initiated configurations

3.9 START-UP RESPONSIBILITY

A. Provide start-up services for systems and equipment in accordance with Access Control General Requirements, Section 28 05 00.

3.10 PRELIMINARY INSPECTION AND TESTING

A. Provide preliminary inspection and testing services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

3.11 SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

A. Provide performance testing, burn-in, and adjusting of systems and equipment in accordance with Section 28 08 00, Testing and Commissioning.

B. Performance Testing

1. Demonstrate the operation of each camera that is associated with EACS monitoring or card reader points.
2. Demonstrate automated call-up, pre-positioning and graphical map control of each camera, from the EACS GUI screens.

3.12 BURN-IN PERFORMANCE PERIOD

A. Provide a burn-in performance period to demonstrate the stability of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.13 COMMISSIONING AND VALIDATION

A. Provide commissioning and validation services to prove and improve the effectiveness of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.14 FINAL PROCEDURES

A. Perform final procedures in accordance with Section 28 05 00, Access Control General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 08 00
SECURITY TESTING AND COMMISSIONING

PART 1 GENERAL

1.1 WORK INCLUDES

A. General Description: This specification section covers the provision of preliminary testing, acceptance testing, burn-in performance testing, and the commissioning of various access control systems at [Indicate Site and Building].

B. Provide Testing to assure that electrical equipment and wiring is operational, within industry and manufacturers tolerances and is installed in accordance with other sections of these specifications.

C. Conduct tests in the presence of the Owner and the Owner's agents for the purpose of demonstrating the equipment or systems' compliance with specifications. Demonstrate electrical and mechanical tests to the Owner and the Owner's agents that the entire installation is functioning properly and that circuits, including power, control, instrumentation, relaying, integration and communication, will function properly and as specified.

D. Furnish, install and maintain tools, instruments, material, test equipment, test connections and power. Furnish personnel including supervision and "stand-by" labor required for the testing, setting, and adjusting of electrical facilities and component parts including putting the above into operation.

E. Make tests with proper regard for the protection of equipment and personnel.

F. Protect equipment from subsequent testing of other equipment and systems after equipment has been tested, checked for operation, and accepted by the Owner.

G. Record test values of equipment, giving both "as-found" and "as-left" for existing conditions.

H. The witnessing of any test by the Owner does not relieve the Contractor of warranties for material, equipment, and workmanship, as specified in the General Conditions.

I. Check circuits for conformance with the wiring diagrams furnished by manufacturers.

1.2 RELATED SECTIONS AND REFERENCES

A. In accordance with Project General Requirements and General Provisions.

B. In accordance with Section 28 05 00, Security System General Requirements

C. In accordance with Section 28 05 53, Identification for Electronic Safety and Security

D. In accordance with Section 28 07 00, Security System Integration

E. In accordance with Section 28 08 00, Security System Testing and Commissioning

F. In accordance with Section 28 13 00, Electronic Access Control System

G. In accordance with Section 28 16 00, Electronic Intrusion Detection System

H. In accordance with Section 28 23 00, Video Surveillance System

I. Inspections and tests shall be performed in accordance with applicable codes and standards including the most current versions of NEC, ANSI, IEEE, NFPA, NEMA and OSHA.

J. International Electrical Testing Association, Acceptance Testing Specifications (NETA ATS), latest edition.

1.3 SUBMITTALS

A. In addition to the requirements of Section 28 05 00, four (4) bound copies of the certified test reports shall be submitted to the Owner within seven (7) days after the completion of the work. The final report shall be signed and include the following information:

1. Summary of the project.
2. Description of the equipment tested.
3. Visual inspection report
4. Description of the tests
5. Pre-Acceptance and Final Acceptance Test results
6. Conclusions and recommendations
7. Appendix including appropriate test forms
8. Identification of the test equipment used

1.4 WARRANTY

A. Provide the work in accordance with Section 28 05 00, Security Systems General Requirements

PART 2 PRODUCTS

A. Not Used

PART 3 EXECUTION

3.1 GENERAL

A. Furnish labor, instruments, products, temporary power, and sufficient materials required for testing at each test.
B. Correct deficiencies found as a result of tests and make replacements or repairs to tested products that are damaged as the result of the tests. This included Burn in Performance report reviews
C. Schedule tests at a time convenient to witnesses thereto or persons affected by the tests.
D. Provide fourteen (14) day written notification to the Owner for test procedures prior to the test.
E. Make records of all tests in a neat and legible form. Identify the equipment or system tested and the test data.
F. Check control, instrumentation, and power cables and conductors for proper connections, workmanship and identification.
G. Test disconnect switches through an open and closed cycle for proper operation, alignment and contact.
H. Additional tests required shall be as outlined under the various Sections of Division 26 and 28.
I. Submit to the Owner certified reports on all tests indicating full compliance with test requirements.

3.2 COORDINATION

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

3.3 WORKMANSHIP

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

3.4 PRELIMINARY INSPECTION & TESTING

A. The primary lead consultant brought on board for the project shall perform preliminary project progress checks throughout each phase of construction i.e.: Demo, Rough-in, and Trim-out.
    1. The Consultant shall coordinate project progress check-ins with the USC Project Manager.
    2. Consultant shall coordinate with Access Control Systems Specialist and Admin OPS IT to be aware of progress project checks.
B. Coordination: Coordinate testing of components of the system in cooperation with other trades.
    1. The USC Project Manager shall coordinate each phase discussed within the testing and commissioning specifications.

2. The Security Integrator shall confirm with the USC Project Manager when a system is completed and pre-tested to begin the testing and commissioning process below.

C. Verification: Prior to performing Preliminary Testing, inspection, and/or final testing procedures, Security Integrator shall insure the following:
   1. Safe and proper operation of all components, devices or equipment, and the absence of extraneous or interfering signals
   2. Proper grounding of devices and equipment
   3. Integrity of signal and electrical system ground connections
   4. Proper powering of devices and equipment
   5. Integrity of all insulation, shield terminations and connections
   6. Integrity of soldered connections and absence of solder splatter, solder bridges, debris of any kind
   7. Proper dressing of wire and cable with labels matching as-build documents
   8. "Wire-checking" of all circuitry, including phase and continuity
   9. Preliminary targeting and setup of video camera assemblies
   10. Mechanical integrity of all support and positioning provisions, i.e.: as provided for video cameras, monitors and any other equipment
   11. Sequencing: If applicable, determine and record the sequence of energizing systems to minimize the risk of damage from improper startup
   12. Proper operation of devices and systems in accordance with specified performance requirements
   13. System is programmed for alarm reporting of each device and associated with the graphical maps
   14. Verify system programming is defined.
   15. Verify with Owner the provided designations for all devices.

D. Perform a Preliminary Inspection and Test to determine the operating status of components and systems prior to Final Acceptance Testing.
   1. Testing Security Equipment, Enclosures, and Cabinets
      a. Test each equipment enclosure for tamper alarm
      b. Test each power supply battery for power loss alarm reporting
      c. Test 120VAC power loss alarm
      d. Test for communication loss with server reporting
   2. Test power stand-by provisions (UPS, battery backup, generator backup)
   3. Testing Electronic Access Control Doors
      a. Doors with Door Position Switch (DPS) and Request to Exit device (REX) shall be tested for:
         1) Door Forced Open alarm is generated when door is opened from unsecured side
         2) Door Held Open alarm is generated when door is held open past its preprogrammed duration after valid REX event
         3) REX shunts alarm on egress
         4) REX does not shunt forced door alarm
      b. Doors with Electrified Exit Device, DPS and REX
         1) Door is locked in secure mode
         2) Door is unlocked by manual command from system workstation
         3) Door is unlocked by time zone
         4) Door Forced Open alarm is generated during secure mode only
         5) Door Held Open alarm is generated during secure mode only
         6) REX shunts alarm on egress during secure mode, for the preprogrammed duration
         7) Door relocks immediately when door closes after valid passage (does not wait for preprogrammed duration)

8) REX does not unlock door
9) REX does not bypass forced door alarm
10) Door relocks on time zone
11) Door relocks during day mode on manual command from system workstation

c. Doors with Automatic door operators
1) Door is locked in secure mode
2) Door is unlocked by manual command from system workstation during secure mode
3) Door is unlocked by time zone
4) Door Forced Open alarm is generated during secure mode only
5) Door Held Open alarm is generated during secure mode only
6) REX shunts alarm on egress during secure mode
7) REX does not unlock door
8) Door relocks on time zone
9) Door relocks during day mode on manual command from system workstation.

d. Doors or Gates with card reader
1) Door unlocks by use of the card reader for programmed unlock time and does not alarm when door is opened
2) Door is locked in secure mode
3) Door is unlocked by manual command from system workstation
4) Door is unlocked by time zone
5) Door Forced Open alarm is generated during secure mode
6) Door Held Open alarm is generated during secure mode
7) REX shunts alarm on egress during secure mode
8) Door relocks immediately when door closes after valid passage (does not wait for preprogrammed duration)
9) REX for door does not unlock door
10) REX for gates does not unlock gate
11) Door relocks on time zone
12) Door relocks during day mode on manual command from system workstation

4. Testing Video Surveillance System
a. Live viewing
1) Verify each camera live viewing at the monitoring workstation is in focus
2) Verify each camera live viewing at Central Command Post is in focus
3) During an alarm event verify camera and pre-programmed views associated with alarm event are displayed at the viewing location(s)
4) Verify camera identification match Owner defined description.

b. Recorded Images
1) Verify each camera viewing of recorded images at the monitoring workstation
2) Verify each camera viewing of recorded images at Central Command Post
3) Verify alarm event is recorded as specified in 28 23 00

5. Duress Switch – Intrusion Detection System
a. Verify switch activation reports to IDS control panel
b. Verify switch activation reports to monitoring station

6. Wireless Alarm System
a. Verify wireless transmitters are activated by their associated alarm devices.

b. Verify transmitted alarms report their individual ID's to their associated alarm receivers from various locations around the area of coverage.
c. Verify each wireless transmitter supervision reports its individual identification to the system.

E. Adjustments and Documentation: After successfully energizing and testing the systems, make adjustments and document the setting of controls, configurations, as applicable. Tabulate all data along with an inventory of test equipment, a description of testing conditions and a list of test personnel.

F. Test Documentation: Create and provide complete test reports documenting the results of the each performed on each device, control panel, power supply, and other elements of the system. Copies of preliminary test data shall accompany copies of performance testing data as part of the Operating and Maintenance submittal.

3.5 PREPARATION FOR ACCEPTANCE (PRIOR TO FINAL INSPECTION)

A. Temporary facilities and utilities shall be properly disconnected, removed, and disposed of off-site.

B. Systems, equipment, and devices shall be in full and proper adjustment and operation, and properly labeled and identified.

C. Materials shall be neat, clean and unmarred, and parts securely attached.

D. Broken work, including glass, raised flooring and supports, ceiling tiles and supports, walls, doors, etc., shall be replaced or properly repaired, and debris cleaned up and appropriately discarded.

E. Extra materials as specified shall be delivered and stored at the premises as directed by the Owner.

F. Preliminary Test reports of each system and each system component, and Record project documents shall be complete and available for inspection and delivery upon completion of each building/phase as directed by Owner.

3.6 ACCEPTANCE TESTING AND ADJUSTING PROCEDURES

A. Purpose: Conduct testing and adjusting procedures to realize and verify the performance criteria specified herein and identified in Preliminary Testing procedures listed above. Successfully demonstrate the acceptable performance of each specified system in the presence of the Owner and Engineer.

B. Scope: Conduct all performance testing, adjustment and documentation procedures to verify and realize compliance with the performance specifications herein. Make available at least one (1) engineer familiar with this work, and all required test equipment for the duration of performance testing verification, at the convenience of the Owner.

C. Acceptance Testing Readiness: Acceptance testing will be performed after the system is installed and pre-tested completely.
1. The Security Integrator shall provide an acceptance testing plan to the engineer for approval before formal testing is to be performed.
2. Once the testing plan has been approved, the Security Integrator shall have successfully tested the system prior to scheduling formal acceptance testing and provided forms with each test for each portal. Security Integrator shall correct any and all deficiencies found at that time.
3. Security Integrator shall submit the results of the completed test before scheduling final acceptance testing with engineer.
4. Acceptance testing will be conducted in accordance with the approved Acceptance Testing Plan with a minimum of testing listed in Preliminary Testing section.
5. Deliver equipment, devices and materials required for the access control work to the site at least fourteen (14) working days prior to the scheduled Completion Date.

6. Install, test and ready all of the access control work for final Acceptance Testing of the Installation ten (10) working days prior to the Completion Date.

D. Acceptance Testing Schedule: Security Integrator shall confirm in writing to the Owner when the system is ready for acceptance testing. Security Integrator shall then schedule a complete Acceptance Test at the convenience of the Owner.

E. Acceptance Testing
   1. Security Integrator shall test and verify the performance of all equipment, systems, interfaces and peripheral equipment in the presence of the Owner, Owner Representatives, and Engineer.
   2. Tests shall be performed in accordance with the requirements of individual systems as specified herein and in related specification sections. Test shall incorporate testing described in preliminary inspection and testing.
   3. Security Integrator shall furnish communication equipment between the field-testing team and the monitoring team.
   4. Security Integrator shall furnish testing forms for each location.

F. An Observation Report will be generated by the reviewing team, Owner representative, Design Engineer and Security Integrator for Contractor to review

G. Correction of Jobsite Observation Report Items: Perform any and all remedial work to correct inadequate performance or unacceptable conditions of, or relating to any of this work, as determined by the Owner within ten (10) working days of the completion date. Corrective work shall be performed at no additional cost to the Owner. Security Integrator shall provide a written report each week of repairs made and plan to complete repairs in progress.

H. Test Documentation: Document all acceptance testing, calibration and correction procedures described herein with the following information:
   1. Performance date of the procedure
   2. The names of personnel conducting the procedure
   3. The equipment used to conduct the procedure
   4. Type of procedure and description
   5. Condition during performance of procedure
   6. Parameters measured and their values, including values measured prior to calibration or correction as applicable

3.7 BURN-IN PERIOD

A. Prior to Final Acceptance by the Owner, the Security Integrator shall be responsible for performing testing and inspections, as specified herein, to verify that the installation equipment and materials are performing in compliance with the specifications.

B. Upon satisfactory completion of Acceptance Testing and inspection, the Owner shall notify the Security Integrator, and the Burn-In Performance Period shall commence.

C. Security Integrator shall obtain weekly reports of alarm events related to this project and make system repairs or corrections to minimize false alarms. A report shall be provided by the Contactor to the Owner indicating corrections required and locations corrected. Engineer may provide additional comments to the report for Security Integrator to review and provide corrective action.

D. A Performance Period of thirty (30) consecutive calendar days of operating without fault in accordance with the specifications, subsequent to testing and inspection, shall constitute a successful Performance Period.

E. Upon successful completion of the Performance Period, the Owner and design team shall meet to confirm Acceptance, and the Final Acceptance Form shall be executed.

F. If a successful Performance Period cannot be accomplished within ninety (90) consecutive calendar days after commencement of the first Performance Period, the Owner reserves the right to find the Security Integrator in default, and

terminate the Contract. In that event, the Security Integrator shall remove the equipment, and the Owner shall not be responsible for any payment whatsoever to the Security Integrator, except for any materials (i.e., wiring) left in place and elected to be reused by the Owner.

G. Obtain system alarm and event reports at a minimum of four (4) times during the burn in period. Review reports with Owner and repair system equipment and/or adjust system parameters as requested by the Owner or required for system performance.

3.8 COMMISSIONING AND VALIDATION

A. Commissioning is a "fine tuning" process used for complex systems that occurs after acceptance testing, during the Burn-In Performance period and before final acceptance. It helps assure that the system performs to its fullest potential, and validates the effectiveness of the total system implementation in relation to the goals of the access control countermeasures program.

B. After the installation and final testing of the system, a Security System Commissioning team will be assembled to validate the best performance of the system under different scenarios. Alarm reports shall be used to verify operation of the system.

C. This process includes participation by the Owner, Contractor, Security Integrator, and the Consulting Engineer. A third party testing agent may also be hired by the Owner to plan, conduct, and verify the Commissioning process.

D. The Security Integrator shall include a minimum of sixteen (16) hours of participation in the commissioning and validation process by a minimum of two (2) employees familiar with the specific project and installation. Security Integrator shall adjust device installation where alarms are determined to be false.

E. Scheduling of Commissioning and Validation testing will be by the Owner, and may occur after the Notice of Completion, but before the end of the Warranty period.

F. Revisions to the configuration and programming of the system which are recommended by the Commissioning Team as a result of validation testing, shall be performed by the Security Integrator under the direction of the Owner, at no additional charge. The Warranty provisions of this specification shall apply to any configuration and programming revisions resulting from the validation testing process.

G. Revisions and improvements recommended by the Commissioning Team which require physical modifications or additions to the approved and accepted system, including the provision or relocation of new equipment, wiring, and installation, shall be treated as additional changes to the contract, and shall be processed as defined in the Project General Provisions. Where such requested work was part of the Security Integrators' original scope of work, as defined in the design drawings and specifications, or in contract revisions and agreements, the Security Integrator shall provide the work at no additional charge.

3.9 FINAL PROCEDURES

A. Perform final procedures in accordance with Section 28 05 00, Security System General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 13 00
ELECTRONIC ACCESS CONTROL SYSTEM

PART 1 GENERAL

1.1 DESCRIPTION

A. This specification section covers the furnishing and installation of a complete expansion to an enterprise-wide, low-voltage, electronic access control system (EACS) to the [Indicate Site and Building]. project.

B. Security Integrator shall furnish and install access control hardware devices, mounting brackets, power supplies, switches, controls, consoles and other components of the system as shown and specified.

C. Security Integrator shall furnish and install access control related software to allow this system expansion. Software includes required license addition for access control readers and electrified portals, workstations, Video Surveillance System (VSS) Integration.

D. Electrical Contractor shall furnish and install outlets, junction boxes, conduit, connectors, high voltage wiring, and other accessories necessary to complete the system installation. Requirements shall be in accordance with Division 26, Electrical.

1.2 PRECEDENCE

A. Obtain, read and comply with General Conditions and applicable sub-sections of the contract specifications. Where a discrepancy may exist between any applicable subsection and directions as contained herein, this section shall govern.

1.3 GENERAL CONDITIONS

A. In accordance with Section 28 05 00, Security System General Requirements

1.4 RELATED WORK

A. In accordance with Section 08 71 00, Door Hardware.

B. In accordance with Section 28 05 00, Security System General Requirements

C. In accordance with Section 28 05 53, Identification for Electronic Safety and Security

D. In accordance with Section 28 07 00, Security System Integration

E. In accordance with Section 28 08 00, Security System Testing and Commissioning

F. In accordance with Section 28 16 00, Electronic Intrusion Detection System

G. In accordance with Section 28 23 00, Video Surveillance System

1.5 APPLICABLE PUBLICATIONS

A. In accordance with Section 28 05 00, Security System General Requirements

1.6 SHOP DRAWINGS & EQUIPMENT SUBMITTAL

A. In accordance with Section 28 05 00, Security System General Requirements

1.7 OPERATING AND MAINTENANCE MANUALS

A. In accordance with Section 28 05 00, Security System General Requirements.

1.8 SERVICE AND MAINTENANCE

A. In accordance with Section 28 05 00, Security System General Requirements

1.9 TRAINING

A. In accordance with Section 28 05 00, Security System General Requirements

1.10 WARRANTY

A. In accordance with Section 28 05 00, Security System General Requirements

1.11 TECHNICAL REQUIREMENTS, ELECTRONIC ACCESS CONTROL SYSTEM (EACS)

A. General

1. The following information is provided to establish the required system performance for the complete operation of the EACS (Electronic Access

Control System. Some of the performance requirements noted herein are supported and supplied by existing systems in concert with new equipment and software which shall be provided by the Security Integrator under this scope of work. Security Integrator shall provide equipment, wiring and software programming at all locations as necessary to provide a complete system as described herein and as shown on the drawings.

2. The access control system components provided under this scope of work shall be compatible with the existing EACS System and shall function as an integral part thereof. The existing EACS system is a PRO-I Lenel OnGuard system, providing access control services, with a Credentialing system providing global credential database services to the EACS. New devices shall be provided, installed, and connected to the existing system through the owner provided LAN.
3. Security Integrator shall be responsible for providing equipment and software to achieve the specified system performance described herein and, by reference, realize absolute and seamless compatibility with the existing system.
4. Security Integrator shall ensure system additions and modifications provided under this scope of work have no negative effect on the existing systems and operations, and no permanent effect beyond that specified or implied by the scope of work unless otherwise noted herein.

B. Purpose
   1. The electronic access control system is designed to monitor and restrict access to specified areas, and to report on the activity and violations of restricted access in those areas.

C. Environment
   1. The system shall be wholly contained within the [Indicate Site and Building]. project, but shall also be fully integrated with the USC campus enterprise access control systems at the PSA Central Command Center, and other remote sites. Refer to the drawings and Bid Instructions to determine the scope limitations for this phase of work.
   2. Central Administrative Post: The system administrative client is located in the CAPS/PSA Central Command Center. Primary system programming, configuration and control shall occur at this location.
   3. Primary Monitoring Post: Primary monitoring of alarms shall take place in the PSA Central Command Center. The console has an EACS Workstation to monitor alarms, manage response to events, and control access throughout the facility.
   4. Not used.
   5. Infrastructure and Connectivity
      a. Local Sites and Buildings: The EACS workstations and controllers shall reside on the building Local Area Network (LAN) or network segment. Coordinate with the Owner on the provision of LAN ports and network rights.
      b. Enterprise: Local LAN networks will be connected to the campus LAN/WAN, to establish EACS connectivity between campus sites and the Command Center. Coordinate with the Owner on the provision of LAN ports and network rights.

D. Attributes
   1. General
      a. The existing EACS is a Lenel OnGuard PRO Series, supporting an unlimited number of access control readers, unlimited number of

inputs/outputs, unlimited number of client workstations, and unlimited number of cardholders.
   b. The system shall comprise electronic access control system field devices located as shown on the drawings and connected together to provide a complete and operational system.
   c. The EACS shall be based on a distributed system of fully intelligent, stand-alone controllers, operating in a multi-tasking, multi-user environment.
   d. The system shall be compliant with the existing USC EACS, and the credentials shall be compliant with the USC issued credentials.
2. Electronic Access Control System Description
   a. The Electronic Access Control System (EACS) is the key central component for managing physical access control and the bridge between physical and logical access control for this project. The system shall provide a variety of integral functions including the ability to regulate access and egress; provide identification credentials; monitor, track and interface alarms; and view, record and store digital surveillance video linked to EACS events.
   b. Descriptions within this section are part of the existing system. Various descriptions herein will be utilized as part of this project.
   c. The EACS shall be able to seamlessly interface with and monitor Controllers, reader interface modules, I/O panels, burglar alarm panels, burglar alarm panel receivers, biometric devices, personal protection devices, intercom systems, fire alarm panels (secondary monitoring only), building management systems and digital video recorders.
   d. The EACS shall be able to communicate with Controllers via RS-485, RS-232, TCP-IP/Ethernet and Dial-up via Modem.
   e. The system utilizes an open architecture where data must reside on a single database on the EACS and must be accessible in real time to every/any EACS workstation connected to the network. The system is configurable to support the following databases: Microsoft SQL Server and Oracle.
3. EACS Software Capabilities: The EACS Software shall support an unlimited number of card readers, input points, video cameras, intrusion detection points, and relay outputs. The EACS database server shall support an unlimited number of cardholders, visitors, and assets limited only by the available memory on the controller. The database server shall also support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space. Client Workstations shall be limited only by the limitations of the operating system server software.
4. EACS Software Functionality: The Security Integrator shall incorporate the following existing application software features and functionality into the new work, and configure the system and devices to make use of these and any other features offered by the application software, as required by the Owner.
   a. Area Access Manager
   b. Time Zones
   c. Access Levels
   d. Temporary Access Levels
   e. Access Groups
   f. Holidays
   g. First Card Unlock
   h. Database Segmentation
   i. Field Hardware Communications

j. Dual Path Field Hardware Communication
k. Multi-Drop Panel Support
l. Area Control
m. Global Input/Output/Event Linkage
n. Cardholder Use Limits
o. Extended Individual Strike Times
p. Extended Individual Door Held Open Times
q. Extended, on Demand, Door Held Open Times
r. Elevator Control
s. Graphical System Overview Tree
t. Alarms
    1) Pre-Alarm
    2) Alarm/Event Logging
    3) Monitor Zones
    4) Alarm/Event Routing
    5) Text Instructions
    6) Customizable Voice Instructions, Customizable Voice Annunciation: The EACS shall allow for a customizable voice annunciation to be associated EACS alarms. The customizable voice annunciation shall allow the System Administrator to record a voice annunciation of unlimited length.
    7) Alarm Attributes
    8) Alarm-Event Mapping
    9) Alarm Masking Groups
    10) Input Control Module (ICM)
    11) Current Status Indication
    12) Color Coding for Alarm Priorities
    13) Pre-Defined "Canned" Alarm Acknowledgment Responses
    14) Alarm Monitoring – Column Display & Configuration
    15) Test Mode
    16) Alarm Filtering
    17) Alarm Masking
    18) On-Line Context Sensitive Help
    19) Sorting Capabilities
u. Device Group Support
v. Scheduling Utility
w. Access Control
    1) Denied Access Attempts Counter.
    2) Card Reader Time Zone Overrides
    3) Card Reader Options
x. Manual Control
y. VSS Interface
z. Real-Time, Dynamic Graphical Maps

5. The Security Integrator shall add new applications, features, functionality, and options specified herein for the new work, and configure the system and devices to make use of these applications, features, functionality, and options, as required by the Owner.

E. Controllers
1. The Controller shall link the EACS Software to all "down-stream" field hardware components. The controller shall provide full distributed processing of access control/Alarm Monitoring rules and operations. A fully loaded and configured controller shall respond in less than one-half (0.5) second to grant or deny access to cardholder.

2. The controller shall continue to function normally (stand-alone) in the event that it loses communication with the EACS software. While in this off-line state, the controller shall make access granted/denied decisions and maintain a log of the events that have occurred. Events shall be stored in local memory, and then uploaded automatically to the EACS database after communication has been restored.
3. Controller shall incorporate the following features:
    a. UL 294, ULC, and CE Certified
    b. Support for Host Communications Speed of 115,200 Kbps for LNL-3300,
    c. Support for Direct Connect, Remote Dial Up, or Local Area Network (LAN) Connection
    d. Support for Dual Path Host Communications - Secondary Path shall be either Direct Connect, or Local Area Network (LAN) Connection.
    e. Include 15 MB of On-Board Memory (LNL-3300)
    f. LAN Support shall utilize RJ45 (10/100baseT) Ethernet Interface
    g. Non-volatile Flash Memory for real time program updates and overall host communications
    h. Support for 2 wire downstream ports. Downstream ports shall be for connecting card readers and data gathering and output control panels via RS-485 multi-drop wiring configuration
    i. Initial base memory download between controller with standard memory from the EACS shall require no more than ten (10) seconds
    j. Support for up to 64 I/O consisting of RIMs, ICMs, and OCMs in any combination desired with a maximum of 32 I/O CM per controller.
    k. Support of multiple card technologies
    l. Supervised Communications between controller and EACS Software
    m. AES 128-bit Symmetrical Block Encryption conforming to the FIPS-197 standard between controller and EACS Software communications driver.
    n. Multi – drop support for up to eight Controllers per EACS communications port
    o. Support of up to eight card formats and facility codes
    p. RS-485 Full Duplex, UL 1076 Grade AA communication channel to the EACS head-end
    q. Integration to other manufacturer's card readers
    r. Uninterruptible Power Supply (UPS) with battery backup of 15 minutes for AC source.
    s. 32-bit Microprocessor
    t. Biometric Interface Support
    u. Any controller downstream serial port shall multi-drop 16 access control field hardware devices using an RS-485 UL 1076 Grade A communication format allowing a distance of 4,000 feet using Belden 9842 cable or equivalent
    v. 12 VAC or 12 VDC input power
    w. Issue Code Support for both Magnetic and Wiegand Card Formats
    x. Individual Shunt Times (ADA Requirement)
    y. Up to Nine Digit PIN Codes
    z. Status LEDs for normal component and communication status

PART 2 PRODUCTS

2.1 GENERAL

A. Product Acceptability: The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified and compatible with the existing USC

system. Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified. Contractor may not use Contractor proprietary interface modules for connections between field devices and controller.

B. Equipment shall have a UL Listed mark on the product.

C. Assemblies shall be approved by a recognized agency acceptable to the City of Los Angeles.

2.2 ELECTRONIC ACCESS CONTROL EQUIPMENT

A. System (Existing): Lenel OnGuard, PRO Edition, Electronic access control system, configured as described herein. No acceptable equal.

B. Software

1. Operating System (Existing): Microsoft Server 2008, Windows 7, or other standard operating system, as required by the proposed system. Version and configuration shall be as recommended by the manufacturer, based upon compliance with these specifications.
2. Executive Access Control (Existing): Lenel OnGuard, PRO Edition Access Control Management Software, configured to provide the functionality described herein. No acceptable equal.
3. Custom/User Configuration: Provide new programming as required to perform alarm, control, interface, map, graphic and database functions described herein.
4. Area Access Manager: Provide Lenel Area Access Manager for this project, to support independent, local configuration features for this building or specific areas within. Security Integrator shall ensure the final design of controller architecture, quantity, and configuration is consistent with establishing Area Access Manager.

C. System Controller Panels: Provide sufficient controllers and input/output boards to meet all requirements of specifications at each building.

1. EACS Controller
   a. Lenel OnGuard, LNL-3300, Intelligent Dual Reader Controller, with 15MB memory, power supply, battery standby, and Communications Module, as described herein. No acceptable equal.
      1) Controller shall have on board LAN connection
      2) Capacity shall be up to 64 devices per controller.
   b. Security Integrator shall review drawings and specifications with the Owner and Engineer, and may propose changes to the topology of the system based on device layout, where such changes improve performance or functionality of the system. The Owner has final authority as to the final approach for system topology.
   c. Controller Connectivity
      1) Controllers shall support connection to the access control LAN/WAN using TCP/IP protocol, and shall also support connection to the manufacturers standard data communications protocol (RS-232, RS-485, or RS-422).
      2) TCP/IP-connected controllers act as a network “gateway”, to re-transmit controller data via the manufacturers standard data communications protocol (RS-232, RS-485, or RS-422), to other EACS controllers. Provide controllers which support the manufacturers standard data communications protocol, RS-232/20ma, as required.
      3) Connectivity shall be monitored by the system and report loss of communications and restoral of communications. Controller shall

retain in memory events and communicate events during loss of communications to the system upon restoral of communications.

2. Equipment Modules: Provide reader, input and output control capacity at each controller location, to meet the requirements of the site configuration.
   a. Single Reader Interface Module: Lenel Model LNL-1300 Series 3, Reader Interface Module, compatible with the selected readers for use by elevator cab reader when more than one floor access is controlled. No acceptable equal.
      1) Door Contact Input
      2) Request to Exit Input
      3) Supports 16 different card formats
      4) Two Form-C relay outputs
      5) RS-485 Communication to the Controller
   b. Dual Reader Interface Module: Lenel Model LNL-1320 Series 3, Reader Interface Module, compatible with the selected readers. No acceptable equal.
      1) Eight Contact Inputs
      2) Request to Exit Inputs
      3) Supports 16 different card formats
      4) Six Form-C relay outputs
      5) RS-485 Communication to the Controller
   c. Remote Input Board: Lenel Input Control Module (ICM), Model LNL-1100 Series 3, with 16 inputs (4-state supervision) and 2 auxiliary relay outputs. No acceptable equal.
   d. Output Board: Lenel Out Control Module (OCM), Model LNL-1200 Series 3, with 16 outputs. No acceptable equal.
3. Where applicable, add: [Star Multiplexer: Provide Lenel Model LNL-8000 Star Multiplexer module where shown, or as required to implement a star topology or to extend effective communication distances.]
4. Controllers and modules shall be mounted within Security Terminal Cabinets (STC). Cabinets shall be suitable for the environment in which it is installed, as recommended by the manufacturer and required by the specifications.

D. Access Control Readers: Provide USC compliant proximity card readers where shown on the drawings and indicated within these specifications. Card readers shall be "single package" type, combining controller, electronics and antenna in one package, in the following configurations:
   1. Non-Contact Multi-Technology Readers
      a. Multi-Technology Reader: Multi-technology contactless reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and be NFC-compatible. The multi-technology contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards meeting the following requirements:
         1) Compatible with the existing HID 125kHz proximity identification media.
         2) Compatible with Secure Mifare and DesFire identification media, including the Configuration allows reader to be enabled to read smart, proximity or both technologies at the same time.
         3) Secure access control data exchange between the smart card and the reader utilizing diversified keys and mutual authentication sequences.
         4) Optimal read range and read speed for increased access control throughput.

5) Suitable for both indoor and outdoor applications.
6) Customizable behavior for indicator lights and beeper.
7) Multi-technology contactless reader shall comply with the ISO 14443 13.56MHz-related standard.
8) Configurable to read data from any compatible 125 kHz technology simultaneously with 13.56 MHz data.
9) Provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.
10) Configurable to provide compatibility with all standard Prox formats up to 37 bits (including Corporate 1000®).
11) Reader firmware may be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided device.
12) Compliant with the SIA AC-01 Wiegand standard.
13) Reader shall provide the ability to transmit an alarm signal via an integrated optical tamper switch if an attempt is made to remove the reader from the wall.
14) Reader electronics shall be enclosed in a full potted assembly, and provided with a quick connect wire harness.
15) Audio/visual indications shall include
    a) An audio beeper shall provide tone sequence to signify: access granted, access denied, power up, and diagnostics.
    b) A light bar shall provide clear visual status (red/green/amber).
16) Multi-technology contactless reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:
17) Operating voltage: 5 – 16 VDC, reverse voltage protected. Current requirements: 160 mA DC, 195 mA PEAK @ 12 VDC
18) Multi-technology contactless reader shall meet the following physical specifications:
19) Color: Black, Gray, Brown or Cream as approved by the project architect.
20) Weatherized design suitable to withstand harsh environments
21) Certified rating of IP65
22) Multi-technology contactless reader cabling requirements shall be:

b. Mullion Mounting
    1) Provide “mullion” mounting style readers near glass doors, where shown on plans.
    2) Reader shall be suitable for indoor or outdoor use.
    3) Provide AptiQ Model MT11, compatible with existing card media. No acceptable equal.
c. Wall Mounting
    1) Provide “single-gang” mounting style readers for wall and stanchion mounting, where shown on plans.
    2) The reader shall have an approximate read range of up to 3” when used with the proximity access card.
    3) AptiQ Model MT15, compatible with existing card media. No acceptable equal.
d. RFID Card Reader/Keypad Combination Assembly

1) Provide Reader/Keypad combination assembly where shown on drawings.
2) The Keypad shall be an integral part of the reader assembly.
3) The reader shall have an approximate read range of .5”-1.2” when used with the compatible access card.
4) Provide Weather Kit when mounting outside.
5) AptiQ MTK15, compatible with the existing card media. No acceptable equal.

e. Biometric Readers
1) Provide Biometric / Reader combination assembly where shown on drawings.
2) The Biometric scanner shall be an integral part of the reader assembly.
3) The reader shall have an approximate read range of .5”-1.2” when used with the compatible access card.
4) The Biometric Scanner shall accommodate up to 500 users and shall be extendable to 3K or 10K users.
5) Provide Weather Kit when mounting outside.
6) MorphoAccess – SIGMA Lite Proximity Series MPH-AC001A, compatible with the existing card media. No acceptable equal.

f. Reader Licenses
1) Provide Lenel block of 64 reader licenses as required.

E. Wireless Access Control Modules
1. Allegion Schlage PIM400-1501 intelligent controller powered by Lenel. No acceptable equal.
a. Controller shall have on board LAN connection.
b. Capacity shall be up to 16 devices per controller but shall not exceed 8 devices per controller.
c. Security Integrator shall review drawings and specifications with the Owner and Engineer and may propose changes to the topology of the system based on device layout, where such changes improve performance or functionality of the system. The Owner has final authority as to the final approach for system topology.

2. Controller Connectivity
a. Controllers shall support connection to the access control LAN/WAN using TCP/IP protocol, and shall also support connection to the manufacturers standard data communications protocol (RS-232, RS-485, or RS-422).
b. Connectivity shall be monitored by the system and report loss of communications and restoral of communications. Controller shall retain in memory events and communicate events during loss of communications to the system upon restoral of communications.

3. Wireless Door Locks
a. Provide wireless door lock and RFID Reader combination assembly where shown on drawings.
b. The reader shall be an integral part of the door lock assembly.
c. The reader shall have an approximate read range of .5”-1.2” when used with the compatible access card.
d. Allegion Schlage AD400 wireless door locks. No acceptable equal.

4. Wireless Access Control Range Extender (Antenna)
a. Provide range extender antenna where shown on the drawings.

b. Security Integrator is to perform a range test prior to installation to confirm communication frequency between the controller and door locks.
c. Wireless range extender is to be located no further than 15' feet from the main controller.
d. Provide Schlage Allegion ANT400-REM-I/O omni-directional flat panel antenna for indoor use. (Wall Mount)
    1) Wireless range extender shall provide up to 200' of extended communication range within a typical building.
    2) Wireless range extender shall provide up to 1000' of extended communication range within a clear line of sight.
e. Provide Schlage Allegion ANT400-REM-CEILING omni-directional antenna for indoor use. (Ceiling Mount)
    1) Wireless range extender shall provide up to 200' of extended communication range within a typical building.
    2) Wireless range extender shall provide up to 1000' of extended communication range within a clear line of sight.
f. Provide Schlage Allegion ANT400-REM-HALL bi-directional antenna for indoor use. (Wall Mount / Ceiling Mount)
    1) Wireless range extender shall provide up to 200' of extended communication range within a typical building.
    2) Wireless range extender shall provide up to 1000' of extended communication range within a clear line of sight.
g. Provide Schlage Allegion ANT400-REM-I/O+6dB directional flat panel antenna for indoor/ outdoor use. (Wall Mount / Post Mount)
    1) Wireless range extender shall provide up to 200' of extended communication range within a typical building.
    2) Wireless range extender shall provide up to 2000' of extended communication range within a clear line of sight.
    3) Outdoor installation requires the MGB+MCA5 grounding kit.

F. Intercoms
1. Intercoms shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and be NFC-compatible. The intercom reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards meeting the following requirements:
    a. Provide Intercom with, Audio, Camera, RFID Card Reader Module, and Touch Display (Optional) where shown on the drawings.
    b. Provide Micro SIP computer software-based Intercom Master Station, where shown on the drawings.
    c. Provide 2N INDOOR TOUCH 2.0 Intercom Master Station stand-alone answering unit where shown on the drawings.
    d. The Intercom RFID module shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and be NFC-compatible.
    e. The Intercom RFID module shall be compatible with the existing HID 125kHz proximity identification media.
    f. The Intercom RFID module shall have an approximate read range of .5"-1.2" when used with the compatible access card.
    g. The intercom shall be equipped with audio for communication between the Intercom and the Intercom Master Station.

h. The Intercom shall be equipped with an integrated camera supporting a 1280 x 960px JPEG resolution and 640 x 480px video call resolution.
i. The Intercom shall be equipped with a touch display to support digital directory. (Optional)
j. Provide Model 2N IP Verso, compatible with existing card media. No acceptable equal.

G. Access Control Terminal Cabinet (STC)
1. System controllers and field control boards serving a given area shall be installed inside Access Control Terminal Cabinets. No controller or control module shall be mounted independently of the cabinet and its power supplies. Refer to the drawings and the following description for details on STC construction.
2. Provide Access Control Terminal Cabinets as described below, located as shown on the drawings, or at places convenient to its respective field devices. STC shall be listed by an agency approved by the City of Los Angeles Department of Building Safety. Each STC shall contain the following equipment to support the current and future alarm initiating and controlled devices to be connected at that STC location:
a. STC Cabinet
1) Life Safety Enclosures
a) Utilize the Life Safety Enclosures following the USC-specific part number.
b) Provide enclosure size as shown on the drawings.
2) Life Safety Enclosures USC Specific Part Numbers:
a) FPO150-B1002D8PM8NL4E6M-WP-USC01 (30"x23"x6.5" (3) BOARD, (6) DOOR ENCLOSURE)
b) FPO150/250-3D8P2M8NL4E8M2-WP-USC02 (36”x30”x6.5” (8) BOARD, (16) DOOR ENCLOSURE)
c) FPO250/250-3D8P5M8PNLXE12M-WP-USC03 (48”x36”x8” (12) BOARD, (24) DOOR ENCLOSURE)
3) Provide door tamper switch and wire into alarm input for each STC cabinet.
b. STC Source Power
1) Derive primary STC 120VAC power from a designated power source in a secure location, or as shown on plans.
2) Power cable shall be protected by conduit.
3) Transformers shall be installed in locked cabinets, protected by tamper switches. Plug-in transformers which are not protected by locked cabinets are not acceptable.
4) Serve all low voltage powered devices within the STC from the Electronics Power Supply.
5) Provide barriers as may be necessary to separate Class I from Class II power.
c. Electronics Power Supply
1) Class II power supplies shall be integrated within the STC.
2) Capacity: The power supply shall be capable of powering a minimum of 125 percent of the load required at the time of acceptance (25% spare capacity).
3) Power Monitoring: The system shall monitor the loss and restoration of power at the STC of both primary and secondary loss of power. Loss and restoration of power shall be displayed at the console, but shall not require resetting of the system.

4) Battery Back-up: Provide battery back-up to retain functions of all electronics for a period of four (4) hours upon loss of 120VAC power.
5) Transformers shall be installed in locked cabinets, protected by tamper switches. Plug-in transformers which are not protected by locked cabinets are not acceptable.

d. EACS Controller Board: As required for connection to Owner LAN, access readers, locks, door position switches and egress devices associated with access-controlled doors.
e. EACS Alarm Input Board: As required for connection to alarm initiating devices shown connected at this location.
f. EACS Output Control Board: As required for connection to controlled devices shown connected at this location.
g. STC Tamper Switch: Provide a tamper switch on the STC. Connect to the system as an individual alarm point.
h. Terminations: Provide connections to labeled screw barrier terminal blocks.
i. Secure devices within the STC. Dress all wiring in a neat and workmanlike manner. Label conductors to match documentation as described within Section 28 05 53.

3. Lenel Controller Cabinets: Lenel CTX enclosures may be acceptable as STC cabinets if they meet the requirements of an STC as described herein.

H. Lock Power Supply (LPS for Latch Retraction Exit Devices)
1. Provide Command Access Technologies, UL Listed power supplies (Model PS480B) within a ventilated, locked cabinet where indicated on the contract drawings, or as otherwise required to affect proper system performance. Cabinet shall be equipped with a tamper switch, which shall be connected to the EACS to provide a supervisory alarm. Power supply shall include separate terminals for each door lock. Power supply voltage shall be as required by the hardware supplied locks.
2. Capacity: The power supply shall be capable of powering 200 percent of the load required at the time of acceptance (100% spare capacity). Provide the appropriate number of output channels to support the installed devices, plus expansion channels.
a. Power supply not to exceed 75% capacity on one LRPS enclosure.
b. Limit six doors landed on terminals per one enclosure.
3. Power Monitoring: The system shall monitor the loss and restoration of power at the STC. Restoration of power shall be displayed at the console, but shall not require resetting of the system.
4. Solid-state inputs and outputs.
5. Battery Back-Up: Power supplies shall be equipped with integral battery recharging circuits and batteries. If a separate cabinet is used for batteries, the cabinet shall be locked and provided with a tamper switch connected to the EACS. Size the batteries in accordance with the following rules.
a. Fail Safe Door Locks: Provide 4 hours of battery backup for low-voltage electrified door hardware.
b. Fail-Secure Door Locks: Provide battery backup sufficient to operate fail-secure door locks 100 times per hour, for four hours.
6. Provide a Fire Alarm Interface Link to interface the LPS to the STC and Fire Alarm System, as shown on the contract drawings.
7. Used with Command Access PM200, PWM200, and MM1 latch retraction device modules, and other compatible lock types.

I. Alarm Initiating Devices

1. Door Position Switch: Door Position Switches shall be furnished and installed by the Security Integrator. The Contractor shall align, prepare and fabricate doors and frames to accept specified door position switches. The Security Integrator shall be responsible for coordinating the installation so systems and hardware operate as specified.
    a. Surface Mounted Door Switch: GRI 4405-A or an approved equal Surface Mounted Magnetic Switch with armored cable. Route armored cable to junction box and permanently secure to box with clamp or set-screws. Use only where flush mounted devices cannot be installed.
    b. Non-fire Rated Doors, Flush Mount
        1) Hollow Metal Doors: GRI: 195-12-G or approved equal Recessed Magnetic Door Switch.
        2) Storefront Doors GRI: 195-12-G or approved equal Recessed Magnetic Door Switch.
        3) Aluminum Storefront Door Nascom: Shark/M or approved equal Recessed Magnetic Door Switch.
        4) Wood Faced Doors: GRI: 195-12-G or approved equal Recessed Magnetic Door Switch.
    c. Fire Rated Doors
        General: Contractor shall coordinate all access control hardware equipment and installation so as to maintain the Fire Rating of each specific door to the satisfaction of the local Authority Having Jurisdiction.
        1) Hollow Metal Doors: GRI: 195-12-G or approved equal Recessed Magnetic Door Switch, approved by UL for use on UL classified fire doors with metal faces, rated up to 3-hours.
        2) Storefront Doors: GRI: 195-12-G or approved equal Recessed Magnetic Door Switch.
        3) Aluminum Storefront Door Nascom: Shark/M or approved equal Recessed Magnetic Door Switch.
        4) Wood Door w/Hollow Metal Frame: GRI: 195-12-G or approved equal Recessed Magnetic Door Switch.
    d. Gates and Roll-Up Doors GRI 4405-A , or equal, with armored cable. Route armored cable to junction box and permanently secure to box with clamp or set-screws.

J. Exit Request Detector:
    1. Coordinate with the door hardware vendor and use the provided Exit Request Touch Bar or integral lock signal switch, as specified in Division 08.

K. Auto Door Actuator Interface Relay: Provide Dayton Model 1FC13N, or equal, with compatible relay base, at automated doors to ensure the EACS approves the credential/PIN/push-plate before the actuator motor is engaged.

L. Provide IDEC RTE series interval timer, or equal, for interface with motorized door Push Plates and the automated door operator. This will be used to provide a functional time extension for the interaction between the EACS and the automated door hardware, to avoid hardware damage and prevent unwanted alarms.
    1. Unit shall be UL listed and operate on 24VDC.
    2. Unit shall mount to UL listed relay socket.
    3. Unit shall mount within the door operator housing.

M. Local Alarm Horn: Security Door Controls Model 400U-SN, or equal, mounted on a single gang wall plate.

N. Door Release Button, Wall Mounted: Provide Schlage Series 620 Heavy Duty Pushbutton, or equivalent by Security Door Controls, momentary contact, green

lighted mushroom pushbutton. Connect button to an EACS input. Program the EACS to unlock the related door, through EACS logic, when the pushbutton is activated.

O. Communications Server Application Hardware: (Equipment and software supplied by CAPS IT, funded by Contractor when required by system expansion)
   1. Manufacturer: HP Proliant (latest generation meeting the requirements) for back end processes
      a. Note 1: Contractor shall confirm with USC CAPS IT the requirement for the COM SERVER for each project. The server configuration will be based on the specific intent for the hardware. The internal configuration for either back end or NVR processes may be different based on the expected utilization of the Lenel server in a given region.
      b. Note 2: Servers are co-located in the university's Network Operations Center and are supported by the Career and Protective Services Information Technology (CAPS IT) staff. Network connectivity to be designed to ensure minimal disruption to existing operations.
      c. Operating System: Windows Server 2008 (or latest generation)
      d. Virus Protection: Symantec Antivirus (latest generation)
      e. Encryption: Verisign Standard SSL, GPG, Secure FTP
      f. Firewall: Symatec Sygate
      g. Backup & Recovery: Veritas Backup Exec
      h. Database Management System (DBMS): Microsoft SQL Server 2008 (or latest generation)

P. Client Workstation
   1. Provide EACS client workstations and Lenel OnGuard monitoring software in the locations shown on the plans, and as noted herein.
   2. The EACS/VSS Client Workstation(s) shall be a Dell or HP desktop computer that meets or exceeds the current Genetec specifications for a High-Performance Video Client PC, with a dual AMD Radeon HD 7470 Video Card (1GB DDR3 DP/DVI) or better. Contractor shall obtain CAPS IT approval before installation.
   3. Provide Lenel approved SMS Client Software.
   4. (2) 24" LED Monitors (must support 1920x1200 minimum)
   5. Audio with speakers, Mulitmedia keyboard with palm rest, 6-button Laser mouse and surge suppression strip
   6. 3-year limited warranty
   7. Windows 7 Professional, or another operating system approved by Lenel and the Owner.
   8. Microsoft SQL Server 2008 or 2005 Client License

2.3 WIRE AND CABLE

A. General: Cables which are not installed in conduit shall be a version of the specified cable rated for use in plenums.

B. System cable: Provide cable as shown below, or as recommended by the Manufacturer.
   1. Composite Plenum Cable (Reader, Lock, Monitor, REX): Arrow Wire ACP-3NS-1SH9MR jacketed Plenum cable with overall shield, including (6) Conductor Shielded 22AWG w/ripcord, 4-Conductor 22AWG w/ripcord, 4-Conductor 22AWG w/ripcord, and 4-Conductor 18 AWG w/ripcord; or equal by Connect Air International (WSEC Comp 2835), with written approval by Owner.
   2. Composite Cable Water-Block Type (Reader, Lock, Monitor, REX): Arrow Wire ACP-3NS-1SH-9DB jacketed cable with overall shield, including (6) Conductor Shielded 22AWG w/ripcord, 4-Conductor 22AWG w/ripcord, 4-Conductor 22AWG w/ripcord, and 4-Conductor 18 AWG w/ripcord; or equal, with written approval by Owner

3. Lock Power, at Double Doors: Arrow Wire 32LE4-8 jacketed Plenum cable, unshielded, 4-conductor 12 AWG (7-strand), unshielded, or approved equal.
4. Request to Exit Cable, at Double Doors: Arrow Wire 32FB4-6, Plenum rated jacket, 4-conductor 22 AWG (7-strand), unshielded, or approved equal.
5. Special Control Cable, at Double Emergency Exit Doors with Power Booster: Arrow Wire 32LE4-8 Plenum rated cable, 4-conductor 12 AWG (19 strand), unshielded, or approved equal.
6. Card Reader Cable for second card reader at same portal: Arrow Wire 31FB6-3, 6 conductor Shielded 22AWG or approved equal.
7. Alarm Monitoring: Belden 6500FE, 1Pair Shielded 22AWG, or equal.
8. Area Motion Detector: Belden 6441FE, 2 Pair Shielded 20AWG, or equal
9. Push Buttons: Belden 6300UE, 2-Conductor 18AWG.
10. Data: Belden 6441FE, 2 Pair Shielded 20AWG, or equal.
11. Horn: Belden 6300FE, 1 Pair Shielded 18AWG, or equal.
12. Network Cable: As required by Owner Infrastructure.

C. Cable installed below grade shall be rated for immersion in water.

PART 3 EXECUTION

3.1 GENERAL

A. In accordance with Section 28 05 00, Access Control General Requirements.

3.2 SPECIAL INSTRUCTIONS

A. Door Hardware Coordination
1. Doors shall not be locked in path of legal egress.
2. Refer to Section 08 71 00 for door hardware requirements and coordination. Security Integrator shall work directly with door hardware supplier to ensure the provision of specified mechanical and electronic functionality.
3. Request-To-Exit Activation: Security Integrator shall configure system such that Request-To-Exit devices and System Controllers will react quickly enough to bypass alarms before a fast-moving individual can reach and open the door. This bypass process shall be evaluated and verified by the Security Integrator on the fully configured and operational EACS system, prior to acceptance testing.
4. Fire Alarm Interface: Electrified locks and strikes which are part of this work and which may be locked in the path of legal exiting, shall be connected to the building Fire Alarm System in accordance with AHJ requirements such that they automatically unlock in the event of activation of the Fire Alarm System. This shall occur whether the activation is a result of a manual pull station, smoke detector or sprinkler flow switch.
    a. A fire alarm "general/common alarm relay" shall be programmed at the fire alarm control panel to activate the EACS interface relays located in each Lock Power Supply cabinet. The Access Control Security Integrator shall research and provide all necessary fire alarm system conduit, wire, hardware and programming to perform the required interface.
    b. This interface shall not depend on the EACS Host or Remote Controllers for its operation. Locate these interface relays electrically ahead of lock power distribution as shown on the drawings. The Security Integrator shall supply and install programmed alarm interface relay(s) with sufficient capacity to control the power supplied to all controlled locks.

B. Access Control and Lock Configuration
1. Secured Doors: Doors equipped with electric locks shall be individually programmed for locking and unlocking at specific times of the day. A valid credential presented at a reader will allow the portal to unlock for a programmed period of time.
2. Stairwell Door Locks

a. Stairwell doors which are locked from the stairwell side shall have the capability to be simultaneously unlocked upon a signal from the Fire Command Center, Fire Alarm Panel, or the Access Control Command Center.
b. Stairwell locking systems shall, in all respects, comply with the requirements of the California Building Code, “Means of Egress”.
c. Security Integrator shall provide clearly labeled switches, in the required locations, to unlock all stairwell doors simultaneously. Coordinate wall or desk mounted switch style, with the Owner and the Authority Having Jurisdiction.
d. This interface shall not depend on the EACS Host or Remote Controllers for its operation. Locate interface relays for each stairwell door electrically ahead of EACS lock control, to independently override EACS control.

3. Upon authorization by card reader or manual means, “door forced” and “door held open” alarms associated with the portal shall be automatically bypassed (prevented from reporting an alarm) for a duration of time that is programmable on an individual door and individual cardholder basis.
4. The door shall re-lock immediately upon closing, after an authorized access, and the bypass duration shall be immediately truncated. A door position switch will be required at every door for this purpose. The same door position switch shall be used to sense the position of the door for “door forced” and “door held open” alarms.
5. Free Egress Authorization
   a. Unless otherwise shown on the plans or described herein, the system shall detect the normal egress of a user at any individual portal and shall bypass any alarm associated with the portal for a duration of time that is programmable on an individual door and individual cardholder basis.
   b. Timing shall be independently programmed for each portal during the initial enrollment process. This function allows extended timing for disabled persons to pass through a portal.
   c. The timing function shall automatically truncate after an adjustable period (0 - 4 seconds) after a portal is closed. This feature allows a subsequent alarm at the portal to be detected, and prevents the portal from being re-opened without an authorized request.
   d. “Request-to-Exit” devices shall be used to signal the system that an individual is ready to exit the secured door. Request-to-Exit devices may include but not be limited to
      1) Integral Lock Handle Signal Switches
      2) Touch Bars (Electro-mechanical or electronic)
      3) Push Bars (Mechanical)
      4) Push Buttons
   e. On doors with integral electro-mechanical locking mechanisms (strikes, electrical panic hardware, or electrical mortise locks), the mechanical action of the door hardware shall enable egress without requiring release of the electrical mechanism. The Request-to-Exit device shall not unlock the door.
   f. On doors with integral electro-mechanical locking mechanisms (magnetic locks), a Request-to-Exit device may have to unlock the door, releasing the electrical mechanism for the programmed duration. Refer to the drawings and details for direction.
   g. On doors with Intercom system, Security Integrator shall interconnect the intercom system door release button to activate the Request to Exit

function and unlock the door. The door release request contact shall be connected to an input on the EACS, such that an event shall be registered into the EACS system indicating this operation.

C. Sequences: Verify each door type sequence at each door with the Owner.
   1. Doors with Door Position Switch (DPS) and Request-to-Exit (REX) devices
      a. DPS and REX contacts shall be wired to EACS auxiliary input. Configure the EACS to mask the associated DPS alarm for a minimum of 45 seconds. Coordinate the required masking duration with the Owner.
      b. EACS shall report a “door forced” alarm any time the door is opened without a valid REX request. The subsequent operation of an associated REX shall not abort a “door forced” alarm already sensed by the system.
      c. EACS shall report a “door-held-open” alarm after the door has been opened and the masking duration has ended.
   2. Doors with Electronic Locking (EL), DPS and REX devices
      a. DPS and REX contacts shall be wired to EACS auxiliary input. Configure the EACS to mask the associated DPS alarm for a minimum of 45 seconds. Coordinate the required masking duration with the Owner
      b. Electronic lock shall be wired to EACS auxiliary output. Configure the EACS to mask the associated DPS alarm during timed or commanded unlock
      c. Electric lock shall be locked and unlocked based on preprogrammed schedules and conditions, and by manual control from the EACS client workstations.
      d. EACS shall not cause an alarm event when door is unlocked
      e. EACS shall report a “door forced” alarm any time the door is opened without a valid REX request. The subsequent operation of an associated REX shall not abort a “door forced” alarm already sensed by the system.
      f. EACS shall report a “door-held-open” alarm after the door has been opened and the masking duration has ended during locked mode
      g. REX device shall not unlock the door
   3. Doors with Card Access Control (CR), EL, DPS and REX devices
      a. CR, EL, DPS and REX devices shall be wired to a door controller board
      b. Electronic lock shall be locked on command from the system at any time
      c. Electronic lock shall unlock during a preset time zone or from the system
      d. Electronic lock shall be unlocked and shall not require use of card reader during timed unlock mode
      e. EACS shall not report activity when door is unlocked
      f. During locked mode Card Reader shall unlock the door, mask DPS preventing alarm
      g. EACS shall report a “door-held-open” alarm after the door has been opened and the masking duration has ended
      h. EACS shall report a “door forced” alarm when any time the door is opened without a valid REX request. The subsequent operation of an associated REX shall not abort a “door forced” alarm already sensed by the system.
      i. REX device shall not unlock door
   4. Doors with Auto-Operators, Proximity CR, EL, DPS and REX devices
      a. Auto-Operator controls, CR, EL, DPS and REX devices shall be wired to a door controller board
      b. Electronic lock shall be locked on command from the system at any time
      c. Electronic lock shall unlock during a preset time zone
      d. EACS shall not report alarm activity when door is unlocked

e. Day mode; proximity card reader shall activate the auto operator to open the door
f. Secure mode;
    1) Card reader, auto operator function, shall activate the auto door operator at all times.
    2) Card Reader shall unlock the door, mask the DPS device preventing alarm and allow use of door open pushbuttons. Electronic lock to be unlocked prior to door open mechanism is engaged. Where auto door equipment is not provided with door open pushbuttons, the door shall automatically open after unlocking
g. EACS shall report a "door-held-open" alarm after the door has been opened and the masking duration has ended during locked mode
h. EACS shall report a "door forced" alarm when any time the door is opened without a valid REX request. The subsequent operation of an associated REX shall not abort a "door forced" alarm already sensed by the system.
i. Use of push plate shall activate the EACS REX, unlock the door and operate the auto door system
j. Door shall report a door held open time when REX (push plate or signal from the door operator) is activated, door is opened from the secured side and the system bypass time has expired during locked mode.
k. Verify interior push plate is operational in both locked and unlocked modes
l. Verify exterior push plate is operational during unlocked mode
m. Verify exterior push plate is non-operational until valid card read during locked mode
n. Verify exterior push plate is operational after valid card read during locked mode
o. Verify door can be manually opened during locked mode from secured side

5. Doors with Auto-Operators, Dual CR (Mag Stripe and Proximity types), EL, DPS and REX devices
    a. Auto-Operator controls, CR, EL, DPS and REX devices shall be wired to a door controller board
    b. Electric lock shall be locked on command from the system at any time
    c. Electric lock shall unlock during a preset time zone
    d. Door shall not report alarm activity when door is unlocked
    e. Secure mode
        1) Magnetic stripe card reader;
            a) Card
            b) Card Reader shall unlock the door, during locked mode, bypass DPS preventing alarm and allow use of door open pushbuttons.
            c) Electronic lock to be unlocked prior to door open mechanism is engaged.
            d) Where door open pushbuttons are not provided the door shall automatically open after unlocking
        2) Proximity card reader, auto operator function, shall open the door at all times.
        3) During secure mode the card reader shall operate as item e above.
    f. EACS shall report a "door-held-open" alarm after the door has been opened and the masking duration has ended during locked mode
    g. EACS shall report a "door forced" alarm when any time the door is opened without a valid REX request. The subsequent operation of an

associated REX shall not abort a “door forced” alarm already sensed by the system.

h. Use of push plate shall activate the EACS REX, unlock the door and operate the auto door system
i. Door shall report a door held open time when REX (push plate or signal from the door operator) is activated, door is opened from the secured side and the system bypass time has expired during locked mode.
j. Verify interior push plate is operational in both locked and unlocked modes
k. Verify exterior push plate is operational during unlocked mode
l. Verify exterior push plate is non-operational until valid card read during locked mode
m. Verify exterior push plate is operational after valid card read during locked mode
n. Verify door can be manually opened during locked mode from secured side

6. Auto Sliding Doors shall operate similar to Doors with Auto-Operators.
   a. Contractor to coordinate and confirm door hardware includes electronic remote door locking control capability.
   b. Verify sliding door break a way feature is not disabled when door is in legal path of egress
7. Exterior Gates
   a. As defined by hardware group. PROVIDE GATE WITH ELECTRIC STRIKE] [PROVIDE GATE WITH ELECTRIFIED MORTISE HANDLE, CR, EL, DPS, REX wired to input/output/door controller board as required by application.
   b. Gate shall operate as described for door with similar access control devices.

D. Electrical Connections to Door Hardware: Wire connections to door hardware pigtail leads shall be made using the manufacturer-provided quick-connect devices, or by Dolphin insulated displacement connectors. Wire nuts and splices are not acceptable.
E. Tamper Devices
   1. Terminal cabinets, equipment cabinets, enclosures, power supply cabinets, exposed wireways, and pull and junction boxes with wire connections or splices shall be equipped with tamper switches programmed to report an alarm.
   2. Junction boxes requiring tamper switches that are associated with an individual alarmed device (such as a door position switch) may report to the respective device alarm point, if end-of-line resistors and the system are configured to support 6-state alarm reporting. Other cabinet and box tamper switches shall report as independent alarm points.
   3. Power Supply/Battery Chargers: Power supply/battery chargers shall be connected to alarm monitoring points to provide an "Event" indication of tamper, power failures and other system troubles.
F. Elevator Work
   1. The EACS shall be able to track which floor (Floor Tracking) was selected by an individual cardholder for auditing and reporting purposes.
   2. Elevator car floor selection shall be individually controlled by means of an access reader within the elevator. Control shall be accomplished by disabling/enabling elevator control buttons within the elevator car with respect to building time schedules and authorization rights unique to each card-holder

3. Review elevator specifications for integration between the EACS and elevator systems.
4. Verify the compatibility and completeness of the proposed hardware and its installation, submit detailed drawings showing the proposed modifications and installation, and provide all equipment and services required to achieve the specified electrical and mechanical performance. Coordinate acceptable hardware, modification and installation techniques with the Architect and the Elevator Contractor.
5. The Elevator Contractor shall provide appropriate traveling cables, elevator controller hardware and software to perform elevator control functions based on access control authorization signals generated by the EACS.
6. Elevator Contractor Provisions:
    a. The EACS shall be equipped with, and programmed to provide, individual floor button outputs to the elevator system upon presentation of an authorized access card. Corresponding inputs must be provided on the elevator control system, for each car and floor button.
    b. The elevator control system shall be equipped with, and programmed to provide, the EACS with individual floor selection outputs upon user selection of floor buttons, after the card is authorized. Corresponding inputs must be provided on the EACS control system, for each car and floor button.
7. Notwithstanding time and authorization scheduling, elevators shall always respond to a call initiated from above the ground floor and shall always allow travel from the initiating floor to the ground floor to permit exiting the building.
8. Elevator Control Operating Modes
    a. Access Mode: In the access mode, the passenger may transit to any floor by stepping onto an elevator and pressing any floor button, except those individual floors scheduled to remain in secure mode.
    b. Secure Mode: In the secure mode, a person desiring to go to any floor above the ground floor shall present a valid access card to the card reader in the elevator car. Once authorized, the passenger may then press any floor button for which he has been granted access and the elevator shall respond to the request. Once pressed, the authorized floor button shall light and remain lit until the elevator travels to the respective floor.
    c. It shall be possible to program access and secure modes on an elevator by elevator and floor by floor basis using the access control system.
    d. Common Modes: Pressing the "call" button on any floor will cause the elevator to proceed to that floor and open its respective doors. Anyone may board an elevator from any floor and travel to the ground level without assistance from the access control system. In this mode, the elevator will not stop on any floor other than the floor of original initiation until its travel cycle is completed by reaching the ground floor. Elevator functions are provided by the Elevator Contractor.
    e. Fire Recall Mode: EACS control over the elevator cars shall be disabled by the elevator controller in the event of a "fire recall" command from the Fire Alarm System. In that event, elevators will be recalled to the first floor or the floor of alternate recall as defined by life-safety requirements. Recall and fire/life-safety control modes are not provided by the EACS
9. Access/Disable Mode: A key-switch within each elevator shall disable the access control system for that elevator only, providing an immediate transfer

to access mode for that elevator regardless of any malfunction of the EACS. This switch shall not depend on EACS system activity for its operation Elevator Call Control

10. Provide access card reader at elevator call buttons. Card reader shall be connected to the elevator operator to prevent elevator call at first floor only.
11. Coordinate location of connection with elevator contractor.

G. EACS Connectivity
   1. Access Control Network: EACS Servers, Client Workstations and Controllers shall reside on the Owners' Local Area (LAN) and/or Wide Area Network (WAN) to allow global event activity and shared data interchange.
   2. Provide and coordinate with Owner IT adequate network "firewalls" to maintain the security of EACS controls and information while connected to shared computer networks and transmission media. Contractor shall coordinate shared resource usage with the Owner, and develop network security schemes acceptable to the Owner to ensure the integrity of the EACS.
   3. LAN Communications & Connectivity, (Integrated CPU's and Controller's)
      a. Provide LAN communications interfaces for the applicable EACS Server, Clients and Controllers to support multiple workstation and integration schemes that are part of this work.
      b. LAN Communications: Security Integrator shall utilize the facility's Local Area Network for EACS connections and interfaces, as shown on the drawings and described herein.
      c. Coordinate with EACS equipment and software manufacturers to provide network interface devices compatible with the established LAN/WAN network.
      d. Coordinate with the USC Information Systems Department to provide servers, EACS clients, network interface devices, bandwidth utilization, and appurtenances acceptable to the Owner.
   4. Controller Communications
      a. Inter-Facility: Between facilities, buildings and controller "groups", the controller network shall be implemented utilizing the access control Owners infrastructure and connectivity, as shown on the drawings and described herein.
      b. Between controllers at an individual location, and between controllers located within the same building, the controller network may be implemented using standard, twisted, shielded copper conductors as approved by the system manufacturer. It is also acceptable for controllers to be LAN connected, regardless of location.

H. Emergency Standby Power
   1. Servers, Computers, Clients, and Other 120VAC Equipment: Provide a UPS with sufficient time for power transfer where the respective buildings have an Emergency Power (EP) source. Where a building EP source is not available, provide sufficient UPS time to allow the system to run for a minimum of 1-Hour, plus (15) minutes to manage the shutdown process.
   2. Low-Voltage Equipment: EACS Remote Controllers, peripheral devices and Lock Power Supplies shall also have their own 4-hour battery back-up systems.
      a. Power back-up may be in the form of direct DC battery power back-up or by 120VAC Uninterruptable Power Supplies (UPS), depending upon equipment requirements.
      b. Lock Power Supplies shall allow fail-secure locks to be operated by the system a minimum of 100 times-per-hour, during this time period. Fail-safe locks shall be maintained for the full 4-hours.

c. Battery back-up systems may be distributed throughout the facility to provide the required emergency power to individual components.
d. Battery back-up systems shall include battery chargers to keep storage batteries at their peak charge.

3.3 ACCESS CONTROL SYSTEM INTEGRATION

A. Provide access control system integration equipment, software and programming, in accordance with Section 28 07 00, Access Control System Integration. In addition, provide specific integration schemes noted.

B. EACS Video Integration

1. Provide a Video surveillance system management solution as an integral part of the EACS environment. Refer to Section 28 23 00, Video Surveillance system.
2. Any alarm or event in the EACS shall have the ability to be associated with a digital video clip, or live view in real time. The VSS shall support user defined pre and post event recording modes
3. Each camera shall be configurable for a 32 alphanumeric character name and shall allow for the setup and adjustment of brightness, contrast, archiving, motion detection, Pan/Tilt/Zoom, on a per camera basis.
4. The VSS shall support VSS PTZ control via the EACS video interface for pan tilt zoom functional cameras.
5. VSS shall not have more than 150 millisecond latency.

3.4 EQUIPMENT, RACK AND CONSOLE INSTALLATION

A. Mount equipment in rooms, consoles, equipment racks, and desktops in accordance with Section 28 05 00, Security System General Requirements.

3.5 GROUNDING PROCEDURES

A. Provide grounding of all systems and equipment in accordance with Section 28 05 00, Security System General Requirements.

3.6 WIRE AND CABLE INSTALLATION PRACTICES

A. Provide wire and cable installation in accordance with Section 28 05 00, Security System General Requirements.

3.7 DATABASE PREPARATION, CHECKING AND ACTIVATION

A. Provide database preparation, checking and activation for systems and equipment in accordance with Security System General Requirements, Section 28 05 00.

B. Security Integrator shall import the existing cardholder database into the new system, as part of this work.

C. Provide the following special programming services:

1. Security Integrator shall research with the Owner, develop and install executive and user software required for the final acceptance of the system as specified herein and on the drawings.
2. Security Integrator shall provide the Owner with forms and instructions to facilitate the gathering and entry of user software data. Forms shall include but not be limited to information regarding cardholder data, access privileges, time schedules, portal groups, access groups, alarm points, tenant/elevator authorization, password protection levels, two-man and anti-passback locations.
3. Default Access control time zones for each building shall be set as follows:
   a. Normal Business 6 AM to 6PM allowing free access through any portal without creating an alarm event
   b. Card Access Only from 6PM to Midnight by card holders with valid cards.
   c. Restricted Access from Midnight to 6AM for authorized card holders only as programmed by USCard or Department of Public Safety

3.8 START-UP RESPONSIBILITY

A. Provide start-up services for all systems and equipment in accordance with Security System General Requirements, Section 28 05 00.

3.9 PRELIMINARY INSPECTION AND TESTING

A. Provide preliminary inspection and testing services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

3.10 SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

A. Provide performance testing and adjusting of systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

B. Electronic Access Control System Testing

1. Test and verify the normal operation of every alarm point in all four states at each alarm panel. Test each alarm point for the alarm function by normal operation of the alarm point.
2. Test and verify the normal operation of the Access Control System for each sequence.
    a. Minimum testing shall include but not limited to:
        1) Valid Card Read (No Alarm)
        2) Electronic lock relock time (Door not opened)
        3) Door held open alarm time (Alarm)
        4) Door forced open (Alarm)
        5) Electronic lock relock on close (Closed within relock time)
        6) REX bypass Alarm on exit
        7) REX does not unlock door
        8) Valid card read during active REX
        9) Associated Camera integration call up during alarm event
    b. Testing shall be recorded on approved forms.
3. Test each door during its programmed secure time period to assure that the system commands the lock to activate, and permits access by valid access card holders within one second from presentation of the access card.
4. Verify egress systems on access-controlled doors work correctly.
5. Verify system integration schemes function automatically and correctly.
6. Verify activity at Client Monitoring Station functions correctly
7. Verify operation of auto-door operation.

3.11 BURN-IN PERFORMANCE PERIOD

A. Provide a burn-in performance period to demonstrate the stability of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.12 COMMISSIONING AND VALIDATION

A. Provide commissioning and validation services to prove and improve the effectiveness of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.13 TRAINING

A. Provide training requirements of Security System General Requirements Section 28 05 00

B. Security Integrator shall provide a minimum of two (2) reprogramming training sessions within twelve (12) months of the final acceptance of the system to modify the user programming.

C. User group training shall include;

1. Building walk-through indicating locations of equipment and their usage
2. User operation of client workstations, including alarm monitoring, manual door override, card reader reports, and along with user group special operational request.

D. Maintenance group training shall include;

1. Building walk through indicating locations of equipment and their usage

2. Location and usage of project specific forms located in the equipment showing relationship between devices and connectivity to the Owners network
3. Trouble shooting procedures
4. Operational usage of the equipment
5. Procedures for obtaining technical service and repair of equipment.

3.14 FINAL PROCEDURES

A. Perform final procedures in accordance with section 28 05 00, Security General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 16 00
ELECTRONIC INTRUSION DETECTION SYSTEM

PART 1 GENERAL

1.1 DESCRIPTION

A. General Description: This specification section covers the furnishing and installation of a complete, low-voltage, Electronic Intrusion Detection System (EIDS).

B. Security Integrator shall furnish and install security hardware devices, mounting brackets, power supplies, switches, control equipment, and other components of the system as shown and specified.

C. Licensed Electrical Contractor shall furnish and install outlets, junction boxes, conduit, connectors, wiring, and other accessories necessary to complete the system installation. Requirements shall be in accordance with Division 26, Electrical.

D. General Conditions: Provide the work in accordance with Section 28 05 00, Security General Requirements.

1.2 PRECEDENCE

A. Obtain, read and comply with General Conditions and applied EIDS sub-sections of the contract specifications. Where a discrepancy may exist between any applied EIDS subsection and directions as contained herein, this section shall govern.

1.3 GENERAL CONDITIONS

A. In accordance with Section 28 05 00, Security General Requirements

1.4 RELATED WORK

A. In accordance with Section 28 05 00, Security System General Requirements

B. In accordance with Section 28 05 53, Identification for Electronic Safety and Security

C. In accordance with Section 28 07 00, Security System Integration

D. In accordance with Section 28 08 00, Security System Testing and Commissioning

E. In accordance with Section 28 16 00, Electronic Intrusion Detection System

F. In accordance with Section 28 23 00, Video Surveillance System

1.5 APPLIED PUBLICATIONS

A. In accordance with Section 28 05 00, Security General Requirements

1.6 SHOP DRAWINGS & EQUIPMENT SUBMITTAL

A. In accordance with Section 28 05 00, Security General Requirements

1.7 OPERATING AND MAINTENANCE MANUALS

A. In accordance with Section 28 05 00, Security General Requirements.

1.8 WARRANTY

A. In accordance with Section 28 05 00, Security General Requirements

1.9 OWNER'S RIGHT TO USE EQUIPMENT

A. The Owner reserves the right to use equipment, material and services provided as part of this work prior to Acceptance of the Work, without incurring additional charges and without commencement of the Warranty period.

1.10 TECHNICAL REQUIREMENTS, ELECTRONIC INTRUSION DETECTION SYSTEM (EIDS)

A. Purpose: The Electronic Intrusion Detection System is designed to monitor security alarm devices, and to report to the University's Campus Security Command Center (PSA) on the activity of security alarm devices throughout the building.

B. Environment
   1. The system shall be wholly contained within [Indicate Site and Building]. Refer to the drawings and Bid Instructions to determine the scope limitations for this phase of work.
   2. Security Alarm Remote Monitoring: System security alarm and trouble signals shall be transmitted to the UPC Campus Security Command Center (PSA) via its integral Digital Alarm Communicator Transmitter, communicating over telephone lines provided by the Owner. Optionally, the Owner may elect to monitor the system through the campus LAN/WAN using TCP/IP protocols. Security Integrator shall coordinate with the Owner on the provision and compatibility of Owner-provided connectivity.

C. Attributes
   1. General
      a. The system shall comprise Electronic Intrusion Detection System field devices including but not limited to intrusion detectors, door position switches, and duress alarm stations, located as shown on the drawings and connected together to provide a complete and operational system.
      b. The EIDS shall be based on a distributed system of individual point monitoring modules, access keypads and alarm control centers (ACC).
      c. The system shall be U.L. listed for Central Station, Local and Auxiliary, and Burglary (UL Central Station and Local) applications and shall be compatible with the Owner's existing alarm receiving station.
   2. System Control Panel and Features
      a. System Software: The base panel shall come complete with the software necessary to implement every system feature and to allow for the addition of every expansion or functional module without changes or addition to the basic software.
      b. The control panel shall support the following:
         1) Integrated Telephone Line Interface with programmable options for signaling and supervision.
         2) Conettix IP based communication option provides high-speed, secure alarm transport and control.
         3) 32 programmable areas with perimeter and interior partitioning.
         4) 8 on-board, class B hardwired points with expansion capability for a total of 599 wired or wireless points.
         5) Compatibility with touch-screen color LCD, vacuum fluorescent, ATM style LCD or LED style Alarm Command Centers.

6) Local or remote programming, test, and diagnostic capability via a computer running the Remote Programming Software (RPS).
7) The system shall support the use of an Apple iOS device for control. Functions to include arming, disarming, control of outputs, lock, unlock, cycle and secure access doors.
8) Integrated real time clock, calendar, test timer and programmable scheduling capability for relay control and automatic execution of system functions based on a time/event.
9) Provide 1.4 amps of power for standby operation and 2 amps of alarm power, both rated at 12 VDC.
10) 2 wet-contact relay outputs and 1 Auxiliary wet-contact relay output with expansion capability for up to an additional 128 dry-contact relay outputs.
11) Integrated battery charger with reverse hook up protection, battery supervision and battery deep discharge protection.
12) Supervision of peripheral devices and communications interface(s).

c. The EIDS shall have the capability to expand up to 599 separately identifiable points, of which 8 are on-board and 591 are off-board wired or wireless addressable points connected to multiplexed backbone trunks via wired modules and/or wireless receivers.
1) The 8 on-board points shall be able to accommodate powered class B functionality using a powered loop interface module.
2) Point Expansion Modules (Wired and Wireless) shall be able to be located remote to the main panel to a maximum distance of 1000 feet.

d. The EIDS shall support 32 independent areas. Each of the 32 areas shall have custom text associated with the armed state, disarmed state and point-off normal state.

e. The EIDS shall be capable of assigning 1 to 32 account identifiers to the areas depending on the distribution of areas per account.

f. The EIDS shall be capable of linking multiple areas to a shared area which may be automatically controlled (hallway or lobby).

g. The EIDS shall accommodate conditional area arming dependent on the state of other areas (master or associate). Any area can be configured for perimeter and interior arming, not requiring a separate area for this function.

3. Alarm Command Centers (System Keypads):

a. The EIDS shall accommodate connection with up to 32 ACCs, each capable of displaying custom English text on touch screen liquid crystal or vacuum fluorescent (VF) displays.

b. The Alarm Command Centers shall accommodate viewing and configuration of system parameters including:
1) Network Parameters:
a) DHCP Enable/Disable for the selected network module.
b) UPnP Enable/Disable for the selected network module.
c) IP Address for the selected network module

d) Subnet Mask for the selected network module.
e) Default Gateway for the selected network module.
f) Port Number for the selected network module - The module's port number shall range from 0 to 65,535.
g) DNS Server Address for the selected module's DNS server IP address
h) DNS Host Name for the selected module. The DNS host name shall contain up to 63 characters.
i) AES Encryption Key Size – Enable/Disable encryption by selecting the AES encryption key size for the selected network module.
j) AES Encryption Key String - The user shall be able to display, add and modify the AES encryption string based upon the key size previously configured for the selected network module.

2) Point Parameters:
a) Point Selection between one and the maximum number of points in the control panel.
b) Point Registration to allow system response from a specific physical point on any one of the expansion modules; On-board, Point expansion modules (wired or wireless), and Access.
c) Wireless points shall be able to be enrolled in the system via an auto learn

3) Event Routing Parameters to allow programming of up to 4 report routing groups as well as configuration of primary and secondary paths.

4. User Codes: Up to 2000 different passcodes shall be accommodated.
5. Supervision: Each zone in the system shall be supervised. The base panel and any remote panel with its own AC input shall be supervised for AC loss. Batteries for the base panel and all remote panels shall be supervised for low power and be short circuit-protected. Each addressable device and each wireless input device shall be supervised for its presence. The communications bus shall be supervised for low voltage and the presence of each enrolled module and keypad. Digital alarm communicators shall be supervised for telephone line trouble and failure to communicate.
6. Network Communication: The EIDS shall be capable of network communications over a LAN, WAN, Intranet, or the Internet. The system shall include supervision of the network communication utilizing configurable periodic heartbeats to the Digital Alarm Communications Receiver (DACR). The DACR shall provide notification of the loss of communications from a networked system after a programmable timeframe since the last communication. The notification options shall be programmable and include local annunciation or indication to automation software.

a. The network interface module shall be capable of supporting Dynamic Host Communication Protocol (DHCP) to obtain an IP Address.
b. The system shall support a method of authentication between the control panel and the receiver to ensure that the control panel has not been compromised or replaced.
c. The network interface modules shall be capable of supporting encryption using a minimum of 128-bit AES Encryption (Rijndael) certified by NIST (National Institute of Standards and Technology).
d. The network interface modules shall support a 10/100BaseT connection to an Ethernet network.
e. The control panel shall be capable of network communication with a programmable poll time to send periodic heartbeats to the receiver, programmable ACK Wait time, and programmable retry time. In the situation where a communication path is unsuccessful, the control panel shall be capable of attempting backup communication through an available communication method to the same receiver or a backup receiver.
    a) The control panel shall have the ability to automatically adjust the heartbeat rate of a backup path that is using GPRS to the heartbeat rate of the primary path in case of a primary path failure. Upon restoral of the primary path, the heartbeat rate of the backup path shall automatically restore to the original rate. This allows a system utilizing GPRS communications to keep the wireless charges low.
    b) The network communication between the control panel and the receiver shall use ModemIIIa^2.
    c) The control panel shall be capable of two-way communication using a wired network interface module with a 10/100BaseT on a LAN/WAN/Internet configuration or with a wireless GPRS module on the Internet.
    d) The control panel shall be capable of configuring the destination of the receiver using a URL or static IP Address.
    e) The control panel shall be capable of using DNS to lookup the IP Address of the receiver when programmed with a URL.
    f) The control panel shall support UPnP for automated Port Forward configuration in the router where the control panel is installed.
    g) The control panel shall support AutoIP to enable the RPS software to connect to the control panel locally using an IP Direct connection.
    h) The control panel shall support configuration of the IP parameters from the keypad eliminating the need for a PC to configure the IP device.
    i) The control panel shall support network diagnostics from a keypad to allow local testing of network connectivity. The

diagnostics should include, Ethernet EIDS connected, gateway configuration ok, DNS lookup operational, and external network connectivity (such as the Internet) operational.

j) The system shall be capable of meeting DCID 6/9 and UL 2050 standards.

7. Relay Output Modules: The EIDS shall be capable of activating 128 additional relay outputs for auxiliary functions based on its classifications (area vs. panel wide). Output Expansion Modules shall be able to be located remote to the main panel to a maximum distance of 1000 feet. 8 relays (Form C) are to be provided per octo-relay module.
8. System shall bear the following listings as necessary to meet the requirements of governing authorities:
   a. UL 50 - Enclosures for Electrical Equipment.
   b. UL 365 - Police Station Connected Burglar Alarm Units and Systems.
   c. UL 609 - Local Burglar Alarm Units and Systems.
   d. UL 864 - Control Units System for Fire-Protective Signaling System.
   e. UL 1610 - Central Station Burglar-Alarm Units.
   f. UL 60950-1 - Information Technology Equipment - Safety.

PART 2 PRODUCTS

2.1 GENERAL

A. Product Acceptability: The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified. Considerations may include but shall not be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified.

2.2 ELECTRONIC INTRUSION DETECTION SYSTEM

A. System Control Panel
   1. Control/Communicator Panel: Bosch model B9512G, with transformer, fire-rated enclosure, battery back-up, modem/TCP/IP interface, and phone line interfaces. Security Integrator shall confirm compatibility with Owner receiver.
   2. Alarm Command Center (ACC): Bosch B920 series programming keypad with 32character alphanumeric display for EIDS programming and display of alarm status, to match Control Panel Manufacturer.

B. Peripheral Control Equipment
   1. Zone Expansion
      a. Provide 8-Zone hard-wired alarm point expander compatible with the proposed control panel, and as required to connect alarm devices shown on the drawings.
   2. Control Point Output Module: Provide Output Module compatible with the proposed control panel, with 8 output relays and a 1-amp auxiliary power supply.
   3. Coordinate configuration requirements with the Owner and provide programming, configuration and interfaces as necessary to provide a complete and operable system.

C. Power Supply
   1. Ratings: Provide UL Listed Class II transformers and power supplies within the System Control Panel, or within an approved equipment cabinet. Plug-in transformers shall be secured onto power outlets and completely enclosed in a locked cabinet. Provide barriers as may be necessary to separate Class I from Class II power.
   2. Capacity: The power supply shall be capable of powering a minimum of 125 percent of the load required at the time of acceptance (25% spare capacity).
   3. Power Monitoring: The system shall monitor the loss and restoration of power. Loss and restoration of power shall be displayed at the Alarm Control Center and the PSA Central Command Center, but shall not require resetting of the system.
   4. Battery Back-up: Provide battery back-up to retain functions of all electronics for a period of twenty-four (24) hours upon loss of 120VAC power.

D. Alarm Initiating Devices
   1. Door Position Switch: Door Position Switches shall be furnished and installed by the Security Integrator. The Contractor shall align, prepare and fabricate doors and frames to accept specified door position switches. The Contractor shall be responsible for coordinating the installation so systems and hardware operate as specified.
      a. Surface Mounted Door Switch: GRI 4405-A or approved equal Surface Mounted Magnetic Switch with armored cable. Route armored cable to junction box and permanently secure to box with clamp or setscrews. Use only where flush mounted devices cannot be installed.
      b. Non-fire Rated Doors, Flush Mount
         1) Hollow Metal Doors: GRI: 195-12-G (3/4") or approved equal Recessed Magnetic Door Switch.
         2) Storefront Doors Nascom shark/MU or approved equal Recessed Magnetic Door Switch.
         3) Wood Faced Doors: GRI: 195-12-G (3/4") or approved equal Recessed Magnetic Door Switch.
      c. Fire Rated Doors
         1) General: Security Integrator shall coordinate all security hardware equipment and installation so as to maintain the Fire Rating of each specific door to the satisfaction of the local Authority Having Jurisdiction.
         2) Hollow Metal Doors: GRI: 195-12-G (3/4") or approved equal Recessed magnetic door switch, approved by UL for use on UL classified fire doors with metal faces, rated up to 3-hours.
         3) Storefront Doors: Nascom shark/MU or approved equal Recessed Magnetic Door Switch.
         4) Wood Door w/Hollow Metal Frame: GRI: 195-12-G (3/4") or approved equal Recessed Magnetic Door Switch.

d. Gates and Roll-Up Doors: GRI: 4405-A or equal, with armored cable. Route armored cable to junction box and permanently secure to box with clamp or set-screws.

2. Duress Button Wired: Provide W Box: 0E-HBMOMSD3T, or equivalent, duress button, mounted under desk or on wall. The Security Integrator shall mount and align devices as shown on the plans. Coordinate final location with the Owner.
3. Duress Button Wireless: Provide Bosch RFPB-SB-A, or equivalent, wireless duress button. The Security Integrator shall mount and align devices as shown on the plans. Coordinate final location with the Owner.
   a. Wireless Duress Buttons are to be tested quarterly upon project completion by the Owner. Owner to coordinate quarterly testing with Department of Public Safety.
4. Window Contacts Wireless: Provide Bosch RFDW-SM-A Wireless surface mount contact, or equivalent, window contact. The Security Integrator shall mount and align devices as shown on the plans.
5. Wireless Receiver: Provide Bosch B810, or equivalent, wireless device receiver. The Security Integrator shall mount and align the receiver to cover the area shown on the plans. The Security Integrator shall be responsible for coordinating the installation so systems and hardware operate as specified.
6. Motion Detector: Provide Area Motion Detectors designed for the area of usage, device is to be Bosch ceiling DS936 360-degree, or wall-mounted equal, by Bosch and shall be furnished and installed by the Security Integrator. The Security Integrator shall mount and align devices to cover the area shown on the plans. The Security Integrator shall be responsible for coordinating the installation so systems and hardware operate as specified.

2.3 WIRE AND CABLE

A. General: Cables which are not installed in conduit shall be rated for plenum use.
B. System Cable: EIDS System Cable shall be WCW 444380 22/4 Unshielded Stranded Plenum, or equivalent, or as recommended by the Manufacturer and approved by the Owner.
C. Cable installed below grade shall be rated for immersion in water.

PART 3 EXECUTION

3.1 GENERAL

A. In accordance with Section 28 05 00, Security General Requirements.

3.2 EQUIPMENT, RACK AND CONSOLE INSTALLATION

A. Mount equipment in rooms, consoles, equipment racks, and desktops in accordance with Section 28 05 00, Security General Requirements.

3.3 GROUNDING PROCEDURES

A. Provide grounding of all systems and equipment in accordance with Section 28 05 00, Security General Requirements.

3.4 WIRE AND CABLE INSTALLATION PRACTICES

A. Provide wire and cable installation in accordance with Section 28 05 00, Security General Requirements.

3.5 DATABASE PREPARATION, CHECKING AND ACTIVATION

A. Provide database preparation, checking and activation for systems and equipment in accordance with Security General Requirements, Section 28 05 00.

B. In addition, provide the following:

1. Required System Programming:
    a. Security Integrator shall research with the Owner, develop and install executive and user software required for the final acceptance of the system as specified herein and on the drawings.
    b. Security Integrator shall provide the Owner with forms and instructions to facilitate the gathering and entry of user software data. Forms shall include but not be limited to information regarding time schedules, alarm points, password protection levels, and reporting schedules.
    c. Program system configuration parameters (hardware and software, zone/circuit numbers, communication parameters).
    d. Program operational parameters such as opening/closing reports and windows, system response text (custom English) displays of events, activation of relays that drive auxiliary devices, and identifying types of zones/loops.
    e. Program passcodes according to the authorities and functions defined by the Owner.
2. Existing Digital Alarm Communication Receiver Configuration:
    a. Security Integrator shall research with the Owner, and coordinate the programming of the existing Digital Alarm Communications Receiver, located in the PSA Central Command Center. The DACR is manufactured by Osborne.
    b. Security Integrator shall be responsible for providing programming information to the Owner's DACR service organization, prior to the completion of the EIDS installation, and shall participate in testing of the DACR system, as a part of the Final Performance Testing.

3.6 START-UP RESPONSIBILITY

A. Provide start-up services for all systems and equipment in accordance with Security General Requirements, Section 28 05 00.

3.7 SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

A. Provide performance testing, burn-in performance period, and adjusting of all systems and equipment in accordance with Section 28 08 00

B. Electronic Intrusion Detection System Testing

1. Test and verify the normal operation of every alarm point in all four states at each alarm panel. Test each alarm point for the alarm function by normal operation of the alarm point, i.e.: for a door position switch, open the door and so forth.
2. Test each intrusion detector during its programmed secure and bypass time periods to assure that it operates by the pre-programmed schedule.
3. Verify system integration schemes function automatically and correctly.
4. Verify activity at the Digital Alarm Communications Receiver is designated as directed by the Owner.

3.8 BURN-IN PERFORMANCE PERIOD

A. Provide a burn-in performance period to demonstrate the stability of the system, in accordance with Testing and Commissioning, Section 28 08 00.

3.9 FINAL PROCEDURES

A. Perform final procedures in accordance with Section 28 05 00, Security General Requirements.

END OF SECTION

USC GUIDELINE SECURITY SPECIFICATIONS
SECTION 28 23 00
VIDEO SURVEILLANCE SYSTEM

PART 1 GENERAL

1.1 DESCRIPTION

A. General Description: This specification section covers the furnishing and installation of a complete expansion to a low-voltage, enterprise-wide video surveillance system (VSS).

B. Security Integrator shall coordinate and furnish licenses, and install VSS hardware devices, mounting brackets, power supplies, servers, workstations, recorders, controls, consoles, and other components of the system as shown and specified.

C. Furnish and install special boxes, cable, connectors, wiring, and other accessories necessary to complete the system installation. Requirements shall be in accordance with the Division 26, Electrical Work.

D. Outlets, junction boxes, pull boxes, conduit, connectors, wiring, and other accessories necessary to complete the system installation, will be provided in accordance with the projects' Division 26, Electrical Work specifications, and coordinated with VSS requirements.

E. General Conditions: Provide the work in accordance with Section 28 05 00, Security System General Requirements.

1.2 QUALIFICATIONS

A. Provide the work in accordance with Section 28 05 00, Security System General Requirements.

1.3 GENERAL CONDITIONS

A. In accordance with Section 28 05 00, Security System General Requirements

1.4 RELATED WORK

A. In accordance with Section 28 05 00, Security System General Requirements

B. In accordance with Section 28 05 53, Identification for Electronic Safety and Security

C. In accordance with Section 28 07 00, Security System Integration

D. In accordance with Section 28 08 00, Security System Testing and Commissioning

E. In accordance with Section 28 13 00, Electronic Access Control System

F. In accordance with Section 28 16 00, Electronic Intrusion Detection System

G. In accordance with Section 28 23 00, Video Surveillance System

H. In accordance with Section 27 32 26, Emergency Phone System.

1.5 APPLICABLE PUBLICATIONS

A. In accordance with Section 28 05 00, Security System General Requirements

1.6 PRECEDENCE

A. Obtain, read and comply with General Conditions and applicable subsections of the contract specifications. Where a discrepancy may exist between any applicable subsection and directions as contained herein, this section shall govern.

1.7 SHOP DRAWINGS & EQUIPMENT SUBMITTAL

A. In accordance with Section 28 05 00, Security System General Requirements

1.8 OPERATING AND MAINTENANCE MANUALS

A. In accordance with Section 28 05 00, Security System General Requirements.

1.9 WARRANTY

A. In accordance with Section 28 05 00, Security System General Requirements

1.10 SERVICE AND MAINTENANCE

A. In accordance with Section 28 05 00, Security System General Requirements

1.11 TRAINING

A. In accordance with Section 28 05 00, Security System General Requirements

1.12 OWNER'S RIGHT TO USE EQUIPMENT

A. The Owner reserves the right to use equipment, material and services provided as part of this work prior to Acceptance of the Work, without incurring additional charges and without commencement of the Warranty period.

1.13 TECHNICAL REQUIREMENTS, VIDEO SURVEILLANCE SYSTEM

A. General
   1. The following information is provided to establish required system performance for the complete operating Video Surveillance System (VSS) system expansion to the University of Southern California (USC) system. Some of the performance requirements noted herein are supported and supplied by existing systems in concert with new equipment and software which shall be provided by the Security Integrator under this scope of work. Security Integrator shall provide equipment, wiring and software programming at all sites as necessary to provide a complete system as described herein and as shown on the drawings.
   2. The VSS components provided under this scope of work shall be compatible with the existing VSS and shall function as an integral part thereof. The existing enterprise wide network video system is manufactured by GENETEC Inc (Security Center).
   3. Security Integrator shall be responsible for providing equipment, licenses and software to achieve the specified system performance described herein and, by reference, realize absolute and seamless compatibility with the existing system.
   4. Security Integrator shall ensure system additions and modifications provided under this scope of work have no negative effect on the existing systems and operations, and no permanent effect beyond that specified or implied by the scope of work unless otherwise noted herein.

B. Purpose
   1. The System shall provide the ability to record images received from cameras located throughout USC facilities in a digital format.
   2. The System shall allow operators to view live and recorded video images in single and multiple-camera formats based on parameters requested by the user.

C. Environment
   1. The system shall be wholly contained within the [Indicate Site and Building] facility shown on the plans, but shall also be fully integrated with the campus enterprise video surveillance systems (EACS) at the PSA Central Command Center. Refer to the drawings and Bid Instructions to determine the scope limitations for this phase of work.
   2. Not used.
   3. Central Administrative Post: The video management service application is located in the PSA Central Command Center. System programming, configuration and control shall occur at this location or as directed by the Owner.
   4. Building Administrative Post: Where applicable, Video Client workstations shall be located as shown on the drawings. Site surveillance, site camera configuration, and review of recorded images shall occur at this location.
   5. Infrastructure and Connectivity

a. The video camera and processing components at each site shall utilize a combination of standard copper cable, fiber optic cable, IP or wireless transmission schemes, depending on individual site conditions.
b. Local Sites: The wired network cameras, network video archivers, and Client Workstations shall reside on the building's local area network (LAN) or network segment. Recording, live viewing, switching, long-term storage, reviewing, and configuration shall be implemented over this infrastructure. Coordinate LAN/WAN requirements for this project with the Owner.
c. Enterprise: Local LAN networks are connected to the USC campus LAN network, to establish VSS connectivity between USC sites and the PSA Central Command Center. Coordinate LAN/WAN requirements for this project with the Owner.

D. Attributes
1. General
a. The Digital Video Management system (DVMS) is existing and is integrated with the EACS System. Refer to Specification Section 28 13 00, Electronic Access Control Software and Section 28 07 00 Security System Integration for coordinating information.
b. The system shall comprise network video archivers, video clients, digital storage devices, router/switches, and ancillary equipment assembled into a fully operating system.
c. Field Components: Field Components shall comprise video cameras, positioning devices, lenses, camera mounts and housings, and other video system devices and wiring as described herein and shown on the drawings.
d. Video Processing Components: Video processing components shall comprise computer video servers, digital storage devices, computer video monitoring stations, and other video processing devices as described herein and as needed to provide the required functionality.
e. Quality: The initial quality/compression parameters shall be set as determined by the Engineer and the Owner at the time of commissioning. Minimum video quality shall be equivalent to 720p, or the selected camera's highest supported resolution, unless otherwise approved by the Owner.
2. Integrated Digital Video Management System
a. The Security Integrator shall incorporate the following existing application software features and functionality into the new work, and configure the system and devices to make use of these and any other features offered by the application software, as required by the Owner.
b. The VSS/EACS (Spec Section 28 13 00) shall support an integrated Digital Video Management recording solution utilizing a Network Video Archivers that provides the following features and capabilities:
1) Seamless integration with the EACS
2) The EACS shall support Digital Network Video Archivers manufactured by the EACS manufacturer and from third party manufacturers.
3) The EACS shall support analog and IP video sources

4) The Digital Video Management Software (DVMS) shall incorporate a modular architecture and be able to support an unlimited number of cameras
5) The DVMS shall be able to simultaneously record and display live video and display recorded video
6) The DVMS shall support both event based and continuous recording
7) The DVMS shall mark all events and they shall be available for playback and or archiving at any time
8) Video events shall be linked to EACS events in the EACS database.
9) Unlimited simultaneous users shall be able to access any video feed from any archiver on the network.
10) User defined profiles for tailored granular access to configuration and operation
11) Independent camera setup for, compression rate, brightness, contrast and other factor setups.

c. DVMS Network Interface
1) The network interface shall allow remote access of the DVMS from anywhere with established connectivity on the LAN/WAN.
2) The DVMS shall have the ability to playback stored video over the LAN/WAN for remote access of video images.

d. EACS Integration
1) Any alarm/event in the EACS shall have the ability to be associated with a digital video clip in real time. The DVMS shall support user-defined pre and post event recording.
2) Each camera shall be configurable for a 32 alphanumeric character name and shall allow for the setup and adjustment of brightness, contrast, archiving, motion detection, Pan/Tilt/Zoom, on a per camera basis.

e. The DVMS shall support the following configuration and customization parameters:
1) Compression percentage
2) Pre and Post event recording, in seconds
3) Active Continuous Archiving
4) Motion Detection Alarms
5) Set Time Lapse Recording
6) Continuous Recording Mode

3. Real Video Time Monitoring: The DVMS/IPDVMS shall allow monitoring of real time video from any Alarm Monitoring client workstation. DVMS and Camera status shall be displayed on a System Hardware Tree.
4. Matrix View: The DVMS/IPDVMS shall support an advanced Matrix View of On-line camera views. Up to 32 channels shall be able to be simultaneously displayed in the video matrix. The 32 channels shall be any combination of Live or Recorded video.
5. Pan/Tilt/Zoom Control from Alarm Monitoring: Video cameras so equipped, shall be capable of pan/tilt/zoom positioning and remote-control functions. Video camera positioning and imaging signals shall be transmitted by LAN networks as described herein, to permit remote viewing and camera control "on demand" on any LAN connected device, from any location, with appropriate software and authorization.

6. Video Camera Groups/Video Camera Tours
    a. The DVMS/IPDVMS shall support camera grouping to allow for video camera tours in the EACS Alarm Monitoring Module.
7. Still Image Capture/Save: During playback or monitoring of video, the System shall have the ability to create and save a still picture.
8. Export Video Clip to File: The VSS shall have to ability to save and export recorded video to a file for the purpose of sharing and reviewing video clips. The start and end times for each video segment shall be user defined.
9. Video Loss Detection: The VSS/EACS shall detect video loss from cameras and activate an alarm.
10. Automated Motion Video Searching
11. System Redundancy: System servers and network video archivers shall be equipped with RAID 6 array hard drives to allow failed hard drives to be "rebuilt" without loss of recorded information. Hard drives shall be hot swap type.

E. Functional Requirements
1. Video Recording Protocols: Initially, configure the system as directed by the Owner, based on the following recording protocol definitions:
    a. Recording Modes:
        1) 10 frames per second (fps) per camera. Cameras shall be continuously recorded at this rate.
        2) Event/Alarm Mode: 15 fps per camera
    b. Compression Codec: H.264
    c. Compression Quality: Compression rates shall always be set at their highest quality. Automatic throttling can be used where network bandwidth is restricted, when approved by the Owner.
    d. Resolution: Cameras should be configured to deliver streams in their highest native resolution.
    e. Motion-Based Recording Modes: Motion detection recording modes may be implemented where directed by the Owner, but assumptions on motion cannot be used to calculate storage capacity.
2. Recording and Retrieval
    a. Provide a minimum hard-disk storage capacity of 60 days of recording for cameras installed as a part of this project. Storage media shall be located in the security equipment room, communications room, security monitoring center, or where shown on the plans. Storage capacity shall be calculated based on the following parameters:
        1) 10 frames per second (fps) per camera, high-quality compression): All cameras, 24-hours per day, 7-days per week, at highest native resolution.
        2) Assume 100% motion and complexity within the viewing area at all times for storage calculations.
3. Forensic Recording: Provide a means of recording video clips for transport such as DAT, DVD, DVD-ROM or USB storage drive, for forensic and evidentiary purposes.
4. Software routines required to accomplish the required functionality will be fully developed, installed, tested and supported by the Security Integrator and Manufacturer. Provide proof of manufacturer certification for any new software provided.

5. Alarm Management
    a. The USP shall support the following Alarm Management functionality:
    b. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
    c. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.
    d. Set the priority level of an alarm and its reactivation threshold.
    e. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
    f. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
    g. Define the time period after which the alarm is automatically acknowledged.
    h. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
    i. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at- once broadcast mode.
    j. Define whether to display the source of the alarm, one or more entities, or an HTML page.
    k. Specify whether an incident report is mandatory during acknowledgment.
6. Alarm Mode
    a. One or more cameras may be associated with a controlled door or gate, or alarm monitored portal or area.
    b. Associated cameras shall be programmed to be automatically pre-positioned and "called" into alarm mode by EACS event commands, to be displayed in full-screen view on a video workstation and recorded in “alarm/event mode”.
    c. The system shall allow an individual alarm input to initiate pre-positioning, viewing and recording sequences of two or more alarm point-associated cameras, simultaneously. When two or more cameras are simultaneously designated for event recording, they shall each be recorded in “alarm/event” mode.
7. Video Storage/Retrieval
    a. Stored video will be time/date stamped and synchronized with the EACS clock.
    b. The system shall retrieve any stored video based on time/date parameters entered by the operator.
    c. The system shall be capable of performing activity detection on stored video. Any recorded video channel may be selected and a zone may be selected within the view of the camera scene. The stored video can then be searched and will only display clips of video that identify motion in the selected zone.

PART 2 PRODUCTS

2.1 GENERAL

A. Product Acceptability: The Products section contains lists of acceptable products. If product substitutions are proposed, they must be made based upon a comparison of equivalence to the product specified. Considerations may include but shall not

be limited to functional, physical, aesthetic and/or interface aspects. The Owner shall be the sole judge of whether or not a submitted substitution is deemed to be "equivalent" to that specified.

2.2 VIDEO SURVEILLANCE (VSS) EQUIPMENT

A. General
   1. Network Video Recorder: To be provided by Owner.
   2. Software
      a. Camera/Video Licenses: Provide additional number of camera licenses equal to the number of cameras shown on the drawings and added throughout the course of the project.
      b. Client Workstations: Provide GENETEC Client Software Application (CSA) to support monitoring, surveillance, and review capabilities and functionality at the client workstations.
   3. Provide VSS Client Workstations where shown on the drawings and described herein.

B. VSS Client Workstation
   1. The VSS Client Workstation(s) shall be a Dell or HP desktop computer that meets or exceeds the current GENETEC specifications for a High-Performance Video Client PC
      a. 4th Generation Intel® Core™ i7-4770 or better. Security Integrator shall obtain CAPS IT approval before installation.
      b. 16 GB of RAM or better
      c. 64-bit operating system
      d. 240 GB Solid State Drive for OS and Security Center applications
      e. GbE network interface card
      f. 2 x NVIDIA® GeForce® GTX 970 4 GB video card
   2. Provide GENETEC approved Video Client Software.
   3. (2) 24" LED Monitors (must support 1920x1200 minimum)
   4. Audio with speakers, Multimedia keyboard with palm rest, 6-button Laser mouse and surge suppression strip
   5. 3-year limited warranty
   6. Windows 7 Professional, or another operating system approved by GENETEC and the Owner.

C. Wall Mounted Monitors
   1. The wall mounted monitors in Operations Building, Operations room shall be Samsung SMT-4032A or equal, 40", Commercial LED Display, or equal. a. Support up to 1,920 x 1,080 resolution
      a. High contrast ratio 5000:1
      b. Fast response time 8ms
      c. HDMI, DVI, VGA, and Component (CVBS Common) video input
      d. Ethernet/RS-232C remote control
      e. Brightness 350cd/m2
      f. Aspect Ratio 16:9
      g. Viewing Angle (H/V) 178°/178°
      h. Display Color 16.7million
      i. Video System NTSC/PAL
      j. Panel Life 50,000hours
   2. Provide Large Size wall mount bracket.
      a. Tilt: -20° ~ 20°

b. Swivel: -20° ~ 20°

3. Coordinate with architect for structural component to support the weight of the monitors on the wall.

D. Network Video Archiver Hardware Platform

1. The Archiver, a device for recording IP based video from IP output cameras or analog cameras that have been converted to IP output, shall consist of a PC Compatible Chassis and other specified components, as shown in the following sub sections that together create the Archiver.
2. The Archiver is existing and will be expanded for storage retention.
3. GENETEC License: Provide One per camera

E. Cameras

1. IP-Ready Cameras
   a. All new cameras shall be IP-ready cameras, unless the conditions of installation or other special requirements dictate that an analog type camera must be used. Any such condition must be submitted for approval, and approved by the Owner, prior to installation.
   b. Where analog cameras are approved and provided, a digital video encoder must be used to convert the analog video signal for distribution and use on the LAN/WAN Network.
2. Exterior/ Interior Integral Dome with Pan/Tilt/Zoom Camera and Lens
   a. The unitized dome/camera assembly shall be an AXIS Q6075-E or current model, compatible with the IPDVMS. The unitized camera/dome assembly shall be a self-contained unit that incorporates an integral color camera, pan-and-tilt motor, zoom lens and receiver/driver.
      1) Be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG.
      2) Operate on an open source; Linux-based platform, and including a built-in web server.
      3) Be equipped with a slot for SD/SDHC/SDXC memory card expansion, supporting memory up to 64 GB - speed class 10.
      4) Utilize a separate power injector allowing the camera and heater/fan functions to be powered over the network cable.
   b. Hardware. The camera shall:
      1) Be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG. Operate on an open source; Linux-based platform, and including a built-in web server.
      2) Be equipped with a slot for SD/SDHC/SDXC memory card expansion, supporting memory up to 64 GB - speed class 10.
      3) Utilize a separate power injector allowing the camera and heater/fan functions to be powered over the network cable.
   c. Video resolution. The camera shall:
      1) Be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG. Operate on an open source; Linux-based platform, and including a built-in web server.
      2) Be equipped with a slot for SD/SDHC/SDXC memory card expansion, supporting memory up to 64 GB - speed class 10.
      3) Utilize a separate power injector allowing the camera and heater/fan functions to be powered over the network cable.

4) The camera shall be able to deliver at least two individually configurable full resolution full frame rate video streams over IP networks.
5) Supported video resolutions shall include:
a) HDTV 720p (1280x720)
b) HDTV 1080p (1920x1080)

b. PTZ Functionality. The camera shall:
1) Be designed to provide at least two video streams in HDTV 1080p (1920x1080) at up to 60 frames per second (60Hz mode) or 50 frames per second (50Hz mode) using H.264 or Motion JPEG.
2) Operate on an open source; Linux-based platform, and including a built-in web server.
3) Be equipped with a slot for SD/SDHC/SDXC memory card expansion, supporting memory up to 64 GB - speed class 10.
4) Utilize a separate power injector allowing the camera and heater/fan functions to be powered over the network cable.

c. The camera shall provide mechanical PTZ functionality
d. The camera shall provide 40x zoom optical zoom.
e. The camera shall provide 12x digital zoom.
f. The camera shall provide total 480x zoom E-flip.
g. The camera shall provide 360° pan.
h. The camera shall provide 0-220 tilt.
i. The camera shall provide pan and tilt speed in the range of 0.05-450/s.
j. The camera shall incorporate guard tour functionality.
k. The camera shall provide more than 255 preset positions.
l. The camera shall incorporate E-flip functionality.
m. The camera shall provide On-screen directional indicator (OSDI) functionality.
n. Provide mounting bracket for conditions at each location.

2. Interior Mini-Dome Network Fixed Position Camera:
a. Cameras shall be AXIS M4216-LV Network Camera or current and approved equal, high quality progressive scan RGB CMOS 1/3” sensor, be equipped with a high quality vari-focal P-Iris control, IR corrected lens provide pictures down to 0.18 lux.
b. Video:
1) Resolution:
a) The camera shall be able to deliver at least two full frame rate video streams of resolutions up to 720p - 1080p over IP networks.
b) Supported video resolutions shall include 2304x1728 to 320x240 (720p – 1080p)
2) Compression:
a) The camera shall support H.264 (MPEG-4 Part 10/AVC) Baseline, Main and Baseline Profile Motion JPEG.
3) Frame Rates:
a) With WDR: 25/30 fps with power line frequency 50/60 Hz Without WDR: 50/60 fps with power line frequency 50/60 Hz.
4) Streaming:
a) Multiple, individually configurable streams in H.264 and Motion JPEG Axis Zipstream technology in H.264.
b) Controllable frame rate and bandwidth, VBR/MBR H.264
5) The camera shall allow for video to be transported over:
a) IPv4/v6

b) HTTP (Unicast)
c) HTTPS (Unicast)
d) RTP (Unicast & Multicast)
e) RTP over RTSP (Unicast)
f) RTP over RTSP over HTTP (Unicast)

6) Image control:
a) Compression
b) Color
c) Brightness
d) Sharpness
e) Contrast
f) White balance
g) Exposure control (including automatic gain control)
h) Exposure zones
i) Backlight compensation
j) Fine tuning of behavior at different light levels
k) WDR - Dynamic Contrast
l) Text and image overlay
m) Mirroring of images
n) Privacy mask
o) Rotation: 0°, 90°, 180°, 270°, including Corridor Format Power requirements:

c. Power over Ethernet according to IEEE 802.3af/802.3at Type 1 Class 3 Max 9.7 W, Typical 5 W.

d. Cameras shall connect to new Power over Ethernet (PoE) compliant network switch indicated on drawings.

3. Interior Dome Network Fixed Position Camera:

a. Cameras shall be AXIS P3268-LV Network Camera or approved equal, high quality progressive scan 1/1.8” image sensor, support WDR with Lightfinder 2.0, and shall provide images down to 0.14 lux in day mode and 0.08 lux in night mode.

b. The camera shall:
1) Provide video streams in 160x90 to 3840x2160 (maximum) resolution at 30 frames per second using H.264 or Motion JPEG.
2) Equipped with Day/Night functionality and remote zoom and focus capabilities.
3) Operate on an open source; Linux-based platform, and including a built-in web server.
4) Equipped with a slot for SD/SDHC memory card expansion.
5) Tamper resistant body.

c. Hardware:
1) Use a high-quality IR-sensitive 1/1.8” progressive scan CMOS megapixel sensor.
2) Equipped with a removable IR-cut filter, providing so-called day/night functionality.
3) Equipped with a high quality 3-9mm vari-focal DC-iris lens providing remote zoom and focus functionality.
4) Provide pictures down to 0.14 lux while in day mode (with IR-filter in use) and down to 0.08 lux while in night mode (with IR-filter removed).

d. Video resolution:

1) The camera shall be able to deliver at least two individually configurable full frame rate video streams of resolutions up to 3840 x 2160 pixels, over IP networks.
2) Supported video resolutions shall include:
   a) 1280x720
   b) 1280x960
   c) 3840x2160

e. Encoding:
1) Support Motion JPEG encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
2) Support H.264 encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
3) Provide independently configured simultaneous H.264 and Motion JPEG streams.
4) Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.264.
5) Provide configurable compression levels.
6) Support motion estimation in H.264.

f. Supported Protocols shall include IPv4/v6, HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, SNMPv1-3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, and DHCP.
1) The camera shall allow for video to be transported over:
2) The camera shall support Quality of Service (QoS) to be able to prioritize traffic.

g. Image control:
1) The camera shall incorporate Automatic and Manual White Balance and an electronic shutter operating at 1/29500 to 2 seconds (with Lightfinder).
2) The camera shall provide Wide Dynamic Range and backlight compensation with automatic and definable exposure zone.

4. Exterior Dome Network Fixed Position Camera:
   a. Cameras shall be AXIS P3268-LVE Network Camera or approved equal, high quality progressive scan 1/1.8” image sensor, support WDR with Lightfinder 2.0, and shall provide images down to 0.14 lux in day mode and 0.08 lux in night mode.

b. The camera shall:
1) Provide video streams in 160x90 to 3840x2160 (maximum) resolution at 30 frames per second using H.264 or Motion JPEG.
2) Equipped with Day/Night functionality and remote zoom and focus capabilities.
3) Operate on an open source; Linux-based platform, and including a built-in web server.
4) Equipped with a slot for SD/SDHC memory card expansion.
5) Tamper resistant body.

c. Hardware:
1) Use a high-quality IR-sensitive 1/1.8” progressive scan CMOS megapixel sensor.
2) Equipped with a removable IR-cut filter, providing so-called day/night functionality.
3) Equipped with a high quality 3-9mm vari-focal DC-iris lens providing remote zoom and focus functionality.

4) Provide pictures down to 0.14 lux while in day mode (with IR-filter in use) and down to 0.08 lux while in night mode (with IR-filter removed).

d. Video resolution:
   1) The camera shall be able to deliver at least two individually configurable full frame rate video streams of resolutions up to 3840 x 2160 pixels, over IP networks.
   2) Supported video resolutions shall include:
      a) 1280x720
      b) 1280x960
      c) 3840x2160

e. Encoding:
   1) Support Motion JPEG encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
   2) Support H.264 encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
   3) Provide independently configured simultaneous H.264 and Motion JPEG streams.
   4) Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.264.
   5) Provide configurable compression levels.
   6) Support motion estimation in H.264.

f. Supported Protocols shall include IPv4/v6, HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, SNMPv1-3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, and DHCP.
   1) The camera shall allow for video to be transported over:
   2) The camera shall support Quality of Service (QoS) to be able to prioritize traffic.

g. Image control:
   1) The camera shall incorporate Automatic and Manual White Balance and an electronic shutter operating at 1/29500 to 2 seconds (with Lightfinder).
   2) The camera shall provide Wide Dynamic Range and backlight compensation with automatic and definable exposure zone.

5. Interior / Exterior Multi Image Panoramic Network Fixed Position Camera:
   a. Cameras shall be AXIS P3727-PLE Network Camera or approved equal, high quality progressive scan 4 x 1/2.8” image sensors, support WDR with Lightfinder 2.0, and shall provide images down to 0.17 lux in day mode and 0.08 lux in night mode.

   b. The camera shall:
      1) Provide 4 video streams in 640x360 to 1920x1080 (maximum) resolution at 30 frames per second using H.264 or Motion JPEG.
      2) Equipped with Day/Night functionality and remote zoom and focus capabilities.
      3) Operate on an open source; Linux-based platform, and including a built-in web server.
      4) Equipped with a slot for SD/SDHC memory card expansion.
      5) Tamper resistant body.

   c. Hardware:
      1) Use 4 high-quality IR-sensitive 1/2.8” progressive scan CMOS megapixel sensor.
      2) Equipped with a removable IR-cut filter, providing so-called day/night functionality.

3) Equipped with a high quality 3-6mm vari-focal DC-iris lens providing remote zoom and focus functionality.
4) Provide pictures down to 0.17 lux while in day mode (with IR-filter in use) and down to 0.08 lux while in night mode (with IR-filter removed).

d. Video resolution:
1) The camera shall be able to deliver at multiple individually configurable full frame rate video streams of resolutions up to 1920 x 1080 pixels, over IP networks.
2) Supported video resolutions shall include:
a) (4) 1920x1080

e. Encoding:
1) Support Motion JPEG encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
2) Support H.264 encoding in a selectable range from 1 up to 30 frames per second in all resolutions.
3) Provide independently configured simultaneous H.264 and Motion JPEG streams.
4) Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.264.
5) Provide configurable compression levels.
6) Support motion estimation in H.264.

f. Supported Protocols shall include IPv4/v6, HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, SNMPv1-3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, and DHCP.
1) The camera shall allow for video to be transported over:
2) The camera shall support Quality of Service (QoS) to be able to prioritize traffic.

g. Image control:
1) The camera shall incorporate Automatic and Manual White Balance and an electronic shutter operating at 1/29500 to 2 seconds (with Lightfinder).
2) The camera shall provide Wide Dynamic Range and backlight compensation with automatic and definable exposure zone.

B. Camera Enclosures
1. Provide enclosure for each camera. Submit enclosure and mounting hardware configuration to the Owner for approval prior to installation.
2. Ancillary hardware shall be provided by Security Integrator if required, and shall be compatible with and comparable in strength to other attached hardware.

C. Camera Enclosure Mounting Hardware
1. Provision for mounting hardware: Security Integrator shall include provision and installation of miscellaneous hardware and mounting extensions at each camera location to provide acceptable viewing performance.
2. Ancillary Hardware shall be provided by the Security Integrator, if required, and shall be compatible with and comparable in strength to other attached hardware.
3. Provide wall mount, pendent mount, or ceiling mount as required by each location.

D. Camera Power Supply (CPS)
1. PoE Cameras: Cameras with direct IP compatibility shall be compatible with Power over Ethernet (PoE) standards, and will utilize PoE power from the

network switch. Security Integrator shall coordinate power provisions with the University.

2. PoE Cameras: Cameras with direct IP compatibility that require additional power not provided by the network switch, will be required to provide a power injector. Security Integrator shall coordinate power provisions with the University.
3. Ancillary Hardware shall be provided by the Security Integrator, if required, and shall be compatible with and comparable in strength to other attached hardware.

E. Uninterruptable Power Supply
1. Provide APC UPS 1500VA USP and Serial Rack Mount Power Supply at each Archiver installed as a part of this project.
   a. Nominal Voltage 120VAC
   b. Output Power Capacity 980 Watts/1440 VA
   c. Efficiency at Full Load 95.00%
   d. Output Frequency (sync to mains) 57 – 63 Hz for 60 Hz nominal input
   e. Sine Wave Waveform Type
   f. Output Connection shall have (6) NEMA 5-15R receptacles
   g. Nominal Input shall be 120VAC
   h. Nominal Input Frequency shall be 50/60 Hz Auto sensing
   i. Input voltage shall be 82 – 144 VAC
   j. Battery shall me maintenance-free sealed Lead-Acid with suspended electrolyte in a leak-proof enclosure
   k. Communications shall be via RS-232 DB-9 connector and USB
   l. Equipment shall have LED status display with load and battery bar-graphs with specific display for On Line, On Battery, Replace Battery and Overload conditions
2. Provide rack mounting hardware for mounting in equipment racks
   a. Equipment shall not exceed 3.50 inches in height (2 RU)
   b. Equipment shall not exceed 18 inches in depth
   c. Equipment shall not exceed 63 lbs. in weight.

F. Wiring
1. General: Cables that are not installed in conduit shall be rated for plenum use.
2. Video:
   a. IP Cameras, Interior or Protected Wiring: For cameras 100 meters or less from the applicable network switch, provide 23 AWG, 4-pair, plenum-rated Augmented Category 6A (CAT6A) cable. Provide Belden part number 10GX13, or equal provided by the Owner.
3. Exposed Camera Wiring: Wiring between camera enclosures and their respective 'J' Box shall be in "Sealtite" flexible conduit. Sealtite shall be firmly affixed to 'J' Box cover plate and camera enclosure. Refer to camera details.
4. Other cable and cable/interface combinations must be pre-approved by both the manufacturer and the Owner, prior to installation.

PART 2 EXECUTION

2.1 GENERAL

A. In accordance with Section 28 05 00, Security System General Requirements.

2.2 SYSTEM CONFIGURATION

A. Camera recording and display configurations shall be arranged via a combination of the Video Directory Server, Network Video Archivers, Video Monitoring Workstations, and LAN/Wireless LAN network.
B. Security Integrator shall coordinate with the Owner to determine the required pre-programmed surveillance and event-initiated configurations.

2.3 SECURITY SYSTEM INTEGRATION

A. Provide Access Control system integration equipment, software and programming, in accordance with Section 28 05 00, Security System General Requirements.

2.4 EQUIPMENT, RACK AND CONSOLE INSTALLATION

A. In accordance with Section 28 05 00, Security System General Requirements.

2.5 GROUNDING PROCEDURES

A. Provide grounding of all systems and equipment in accordance with Section 28 05 00, Security System General Requirements.

2.6 WIRE AND CABLE INSTALLATION PRACTICES

A. Provide wire and cable installation in accordance with Section 28 05 00, Security System General Requirements.

2.7 DATABASE PREPARATION, CHECKING, AND ACTIVATION

A. Provide database preparation, checking and activation for systems and equipment in accordance with Security System General Requirements, Section 28 05 00.

2.8 START-UP RESPONSIBILITY

A. Provide start-up services for all systems and equipment in accordance with Security System General Requirements, Section 28 05 00.

2.9 PRELIMINARY INSPECTION AND TESTING

A. Provide preliminary inspection and testing services for systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.

2.10 SYSTEM PERFORMANCE TESTING AND ADJUSTING PROCEDURES

A. Provide performance testing, burn-in, and adjusting of systems and equipment in accordance with Testing and Commissioning, Section 28 08 00.
B. VSS Performance Testing
    1. Demonstrate acceptable picture quality and camera views on each camera.
    2. Demonstrate acceptable picture quality on each video monitoring workstation, and display devices accessible over the Wireless LAN.
    3. Demonstrate no negative effects on of video image is observed while Pan-Tilt-Zoom cameras are being repositioned.
    4. Demonstrate switching, recording and playback functions for the video server, and digital video recorders.
    5. Demonstrate camera positioning functionality, on pan/tilt/zoom cameras, throughout the entire range of possible camera positions.
    6. Ensure primary views are acceptable. Demonstrate the view obtained by each preprogrammed camera position.
    7. Demonstrate automatic event-initiated recording sequences, including camera prepositioning, where applicable.

2.11 BURN-IN PERFORMANCE PERIOD

A. Provide a burn-in performance period to demonstrate the stability of the system, in accordance with Testing and Commissioning, Section 28 08 00.

2.12 COMMISSIONING AND VALIDATION

A. Provide commissioning and validation services to prove and improve the effectiveness of the system, in accordance with Testing and Commissioning, Section 28 08 00.

B. Coordinate with the Owner, or the Owner's representative, for the provision of these services.

2.13 FINAL PROCEDURES

A. Perform final procedures in accordance with Section 28 05 00, Access Control General Requirements.

END OF SECTION