South Orange County Community College District

Saddleback College Swimming Pool Refurbishment Project

Bid 5978-2022

Addendum No. 3

10/20/2022

Nick Newkirk
Purchasing and Contracts Manager

Note:
All project documents including contract documents, drawings, and specifications, shall remain unchanged with the exception of those elements added, revised, deleted, or clarified by this addendum.

1. The RFI deadline ended Monday, October 3, 2022 at 5:00 PM. The responses to all RFI's have been released in the PlanetBids system.

2. The Architect's Addendum 1 dated October 3, 2022, is attached to this Addendum.

Bid 5978-2022 Saddleback College Swimming Pool Ref...

Q&A Deadline *October 3, 2022 5:00 PM (PST)*

Set 1 Released via Addendum 3 10/20/2022 12:30 PM (PST) – 10 questions

1.1 Please confirm if field office trailer is required for this project and if one is required for additional use by district personnel.

Answer Although a Contractor's Office is called out in Specification Section 01 52 13, Field Offices and Sheds, one is not required. Similarly, a field office trailer is not needed for District personnel.

1.2 Detail 1 on sheet MR.3 notes new or existing housekeeping pad. Please confirm if new concrete pad is required for new filters for competition and therapy pools

Answer For existing equipment being replaced with new equipment, it is up to the discretion of the contractor to build a new pad or retrofit existing in accordance with Detail 7 on Sheet MR.3. For any other condition, a new pad is required.

1.3 Please confirm that gutter replacement to determined once existing plaster is removed. Please clarify if work is to addressed via change order or provide length of gutter to assume to replace

Answer Pursuant to note 7 on Sheet SP/1, the contractor is to clean, repair and waterproof the exiting therapy pool gutters(s) per Specifications. Reference is to be made to Specification Section 13 11 04, swimming pool ceramic tile for specific scope of work.

1.4 Sloped entry of pool is shown on plans (sheet SP.2) to only be tiled in first 7' of entry. Existing conditions shows full tile entire sloped entry path. Please clarify what areas are to receive new anti slip tile at sloped entry.

Answer Correct Sheet SP.2 for the sloped tile entry to have 10' of tile on ramp so that all dry or potentially dry areas of the ream are finished in the specified tile.

1.5 Plans note to replace eyeball inlets as required. Please confirm all fittings are present, please clarify model to be used for replacement, if required.

Answer Contractor to assume replacement of all eyeball inlets with comparable Pentair,

Hayward, or CMP product.

1.6 Note 18 on sheet SP.1 has call out for plan reference to show on sheet SP.5. Detail does not exist and detail 8 on sheet SP.4 makes not detail note of structural modifications required to step entry, please clarify and provide detail.

Answer The reference to Detail 1/SP.5 on Note 18 on sheet SP.1 should be deleted and replaced with the following callouts: 1/SP.2 Therapy Pool Layout Plans and 8/SP.4 (E) Handrail Details to clarify the scope of the stair entry at the Therapy Pool.

1.7 Note 5 on sheet SP.1 conflicts with specifications, be clarify if these items are required to be included in base bid.

Answer Note 5 on sheet SP.1 may be deleted in its entirety. Contractor to comply with Specifications Sections 01 50 00 Temporary Facilities and Controls and 13 11 00 Swimming Pool General Requirements. Contractor is allowed to connect to local power and water connections if available at no cost to the Contractor; submetering will not be required.

1.8 Please confirm note 6 on sheet SP.1 will be addressed as a change order or provide quantity and size of locations to be bid. These conditions are unknown and unable to quantify until existing plater is removed.

Answer All bidding contractors were required to be present at the mandatory pre-bid conference on September 27, 2022 where they had time to review existing conditions. Further, there was nothing preventing the contractor coming back to site for a follow-up site inspection. If a quantity cannot be determined, the Contractor should assume full replacement of items.

1.9 Can a C-53 Contractor bid this project direct or are they required to subcontract out to a A or B licensed contractor?

Answer The District has modified the Contractor's License Required to be a B or C-53.

1.10 According to the Notice Calling for Bids the project license requirement is open to either an A or B and C-53. My question is can a B license contractor subcontract out the C-53 portion of work or does he have to carry the C-53? Please advise.

Answer The District has modified the Contractor's License Required to be a B or C-53.

Date: October 3, 2022

ADDENDUM 01
To Project Bidding Documents for:

SADDLEBACK COLLEGE
SWIMMING POOL REFURBISHMENT DSA Appl. No. 04-120421
SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT DSA File No. 30-C5

tBP Project No. 21057.00

tBP/ARCHITECTURE
4611 Teller Avenue
Newport Beach, CA 92660
949-673-0300

TO: PROSPECTIVE BIDDERS

This Addendum forms a part of the Contract Documents and modifies the original Bidding Drawings and Specifications dated November 09, 2021. Acknowledge receipt of this Addendum in space provided on the Bid Form. Failure to acknowledge may subject Bidder to disqualification.

CHANGES TO SPECIFICATIONS

1. SECTION 28 13 02 – PHYSICAL ACCESS CONTROL SYSTEM
    a. Add SECTION 28 13 02 issued with this addendum.

ATTACHMENTS

The following attachments are a part of Addendum 01:

1. **Specification Sections**

    SECTION 28 13 02 PHYSICAL ACCESS CONTROL SYSTEM

Gary Moon
tBP/Architecture

Stephen R. Zajicek
FBA Engineering

SECTION 28 13 02
PHYSICAL ACCESS CONTROL SYSTEM

PART 1 - GENERAL

1.01 INTENT

A. It is the intent of South Orange County Community College District to enter into a contract with a qualified contractor to have that contractor procure, provide, install, and make fully operational a Physical Access Control System (PACS) with operational characteristics and capabilities which meet or exceed the product specification and technical performance parameters contained within this document and shown on the Project Drawings.

B. This PACS shall be installed as shown on the project Drawings and described within these Specifications.

1.02 RELATED DOCUMENTS

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

B. Division 8 Section “Door Hardware” for hardware to the extent not specified in this Section.

C. Division 8 Section “Access Control Hardware” for access control to the extent not specified in this Section.

D. Section 28 13 01 Video Surveillance System

1.03 REFERENCES

A. References: Refer to the version year adopted by the Authority Having Jurisdiction.

1. ANSI A117.1 - Accessible and Usable Buildings and Facilities.
2. ICC/IBC - International Building Code.
3. NFPA 70 - National Electrical Code.
4. NFPA 80 - Fire Doors and Windows.
5. NFPA 101 - Life Safety Code.
6. NFPA 105 - Installation of Smoke Door Assemblies

B. American National Standards Institute (ANSI)/Builders Hardware Manufacturers Association (BHMA).

1. ANSI/BHMA A156.10 American National Standard for Power Operated Pedestrian Doors.
2. ANSI/BHMA A156.19 Standards for Power Assist and Low Energy Power Operated Doors.

C. Underwriters Laboratories (UL).

1. UL Listed R-9469 Fire Door Operator with Automatic Closer.
2. UL10C - Positive Pressure Fire Tests of Door Assemblies.
3. UL 325 Standard for Safety for Door, Drapery, Gate, Louver and Window Operators and Systems.
4. UL991 Listed - Tests for Safety-Related Controls Employing Solid-State Device.

5. UL244A - Solid - State Controls for Appliances.
6. UL1998 - Software in Programmable Components.
7. UL1310 - Class 2 Power Units.

D. American Association of Automatic Door Manufacturers (AAADM).

E. American Society for Testing and Materials (ASTM).
1. ASTM B221 Standard Specification for Aluminum and Aluminum Alloy Extruded Bars, Rods, Wire, Profiles and Tubes.
2. ASTM B209 Standard Specification for Aluminum and Aluminum Alloy Sheet and Plate.

F. American Architectural Manufacturers Association (AAMA).
1. AAMA 611 Voluntary Specification for Anodized Architectural Aluminum.

G. National Association of Architectural Metal Manufacturers (NAAMM). 1. Metal Finishes Manual for Architectural Metal Products.

H. International Code Council (ICC).
1. CBC: California Building Code.

1.04 SUMMARY

A. Section includes a physical access control system consisting of credentials, credential creation station, hardwired integrated locksets (with integral proximity card and magstripe readers, door position sensor and request to exit reader), wireless integrated locksets/ panel interface modules (with integral proximity card and magstripe readers, door position sensor and request to exit reader), intermediate controllers and other required and associated hardware and the system headend / software.

B. Physical access control system shall be integrated with systems specified in:
1. Section 27 05 00 Requirements for Communications
2. Section 28 23 02 Video Surveillance System

1.05 DEFINITIONS:

A. Activation Device: Device that, when actuated, sends an electrical signal to the door operator to activate the operation of the door.
1. Knowing act: Consciously initiating the opening of a power operated door using acceptable methods including wall mounted switches such as push plates and controlled access devices such as keypads, card readers and key switches.

B. Access Level: An authorization level or security criteria that must be met before access to a controlled space is granted

C. Access Point: A point of entry into a secure area, typically managed by a door controller and a card reader.

D. ACS: Access Control System

E. API: Application Programming Interface

F. Credential: A card, token, keyfob, or other item which is encoded with information specific to an individual

G. Door Controller: Device which integrates and access-controlled point to the system headend

H. DGM: Dynamic Graphical Maps

I. Double Egress Doors: A pair of doors that swing with the two doors moving in opposite directions and no mullion between them.

J. Encoder: A device utilized to record data onto an access credential

K. Fail Safe Access Point: A door that will unlock automatically in the event of a power failure to permit entering and exiting through the door.

L. Fail Secure Access Point: An access point that automatically locks during a power failure, preventing anyone from entering, but allowing them to exit during an emergency.

M. Input/Output (I/O) Device: An I/O device facilitates elevator control and multi-door monitoring (in/out only).

N. IP-based Access Control: IP access control technology utilizes the network to provide secure network-controlled access and management of physical doors at a facility or location.

O. PACS: Physical Access Control System

P. PDF: Portable Document Format. The file format used by the Acrobat document-exchange system software from Adobe.

Q. Proximity Card (Prox Card): A access control credential that is encrypted with proximity technology and can be read by a proximity reader without having to physically insert the card into the reader, to grant a cardholder access to a location.

R. Power over Ethernet (PoE): PoE carries both power and data for the access control door controller and peripheral door hardware.

S. PoE Injector: A Power over Ethernet (PoE) injector brings PoE capabilities to non-PoE network links.

T. Request to Exit Sensor (REX): A button or device that must be activated to release the door to exit without triggering a forced door alert. Can be stand alone or part of an integrated lockset.

U. Safety Device: A device that detects the presence of an object or person within a zone where contact could occur and provides a signal to stop the movement of the door.

V. SDK: Software Development Kit

W. SSM: Server Software Module

X. SMA: Software Maintenance Agreement

Y. Smart Card: An access card that can be integrated with different technologies including biometric, magnetic stripe, proprietary proximity—and has a memory feature which can contain information about the cardholder.

Z. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

AA. UI: User Interface

BB. UPS: Uninterruptable Power Supply

CC. VMS: Video Management System

DD. WAN: Wide area network.

EE. WMP: Windows media player.

FF. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card.

GG. Windows: Operating system by Microsoft Corporation.

HH. Workstation: A PC with software that is configured for specific, limited security-system functions.

1.06 ACTION SUBMITTALS

A. Product Data: For each type of product indicated. Include dimensions and data on features, performance, electrical characteristics, ratings, and finishes.

B. Shop Drawings: For physical access control system. Include plans, elevations, sections, details, and attachments to other work.

1. Detail equipment assemblies and indicate dimensions, weights, loads, required clearances, method of field assembly, components, and location and size of each field connection. Show means and methods of attachment to all structures, poles, etc.

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

3. Dimensioned plan and elevations of equipment racks, control panels, and consoles. Show access and Workspace Requirements.

4. UPS: Sizing calculations.

5. Wiring Diagrams: For power, signal, and control wiring.

C. Design Data: Include an equipment list consisting of every piece of equipment by model number, manufacturer, serial number, location, and date of original installation.

1.07 INFORMATIONAL SUBMITTALS

A. Field Quality-Control Reports.

B. Product Warranty

1.08 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For integrated locksets, intermediate controllers/ hardware and all other PACS hardware/software components include all operation, troubleshooting, and maintenance manuals. In addition to items specified above, include the following:

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

1.09 QUALITY ASSURANCE

A. Door Hardware IP-Enabled access control products are required to be supplied and installed only through designated ASSA ABLOY "Authorized Channel Partner" (ACP) and “Certified Integrator” (CI) accounts and IMRON authorized dealers. List of ASSA ABLOY and IMRON approved vendors.

B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified Testing Agency, and marked for intended location and application.

C. Comply with NECA 1.

D. Comply with NFPA 70.

E. Electronic data exchange between PACS and video surveillance system shall comply with SIA TVAC.

1.10 WARRANTY

A. Warranty: Contractor's standard form in which Contractor agrees to repair or replace all components of the PACS and/or any other associated device or appurtenance required for full PACS functionality which was installed or provided as a part of this contract, that fail in materials or workmanship within specified warranty period.

1. Warranty Period, Parts and Labor: 1-year from date of system completion and full acceptance.
2. Contractor shall provide pricing for optional extended Parts and Labor warranty for years 1, 2, and 3 post warranty.

PART 2 - PRODUCTS

2.01 QUALITY ASSURANCE

A. Manufacturer of any major component or system installed as a part of this project and not named as a basis of design shall have been in the business of manufacturing such component or system for a minimum of 5 years immediately preceding the date on this document.

B. Any major component or system installed as a part of this contract and not named as a basis of design shall have been installed in a minimum of 3 successfully completed projects of a similar size and scope. Contractor shall supply reference information with their proposal including project name, project location, and contact information for the system end-user.

2.02 BASIS OF DESIGN

South Orange County Community College District has standardized on various systems and equipment to assure compatibility with existing systems and to provide for ease of training as well as more efficient maintenance and spare parts support. As such, items named below as the basis of design shall be considered to have no equivalent

2.03 DOOR HARDWARE MANUFACTURER

Manufacturer: ASSA ABLOY Entrance Systems, 1900 Airport Road, Monroe, NC 28110.

Toll Free (877) SPEC-123. Fax (704) 290- 5555

Website www.assaabloyentrance.com • contact: specdesk.na.aaes@assaabloy.com

2.04 PACS FIELD DEVICES BASIS OF DESIGN TECHNICAL PERFORMANCE SPECIFICATIONS

A. Card Reader - IP Enabled Power-over-Ethernet (PoE) Integrated Card Reader Mortise Lock: IP enabled ANSI/BHMA A156.13 Grade 1 mortise lockset with integrated credential reader, request-to-exit, and door position signaling in one complete unit. Motor driven locking/unlocking control of the lever handle trim, ¾-inch projection latch bolt, and optional 1-inch steel deadbolt.

Lock is U.L listed and labeled for use on up to 3-hour fire rated openings. Available with or without keyed high security cylinder override.

1. Completely intelligent and integrated locking unit with Ethernet power and communication connection capability directly from the locking unit back to the central system host server without additional access control interfaces or components (excluding PoE Endspan and Midspan devices) via an existing or newly installed IEEE 802.3af PoE enabled network.
2. Open architecture design supports wired integration with third party access control systems applications via software development kit (SDK). Real-time software accessible alarms for forced door, unknown card and door held open, with inside lever handle (request-to-exit), battery status, tampering, and door position (open/closed status) monitoring.
3. 2,400 users and 10,000 event transaction history (audit trail). Distributed intelligence allows standalone operation in absence of network communication allowing for system operational redundancy.
4. Provide a network and lock configuration CD tool kit for initial lock setup and programming via a USB connection.
5. Energy Efficient Design: Provide lock bodies which have a holding current draw of 15mA maximum and can operate on either 12 or 24 volts. Locks are to be field configurable for fail safe or fail secure operation.
6. Integrated reader supports the following credentials:
    a. 125kHz proximity credentials: HID, AWID, and EM4102.
    b. 13.56 MHz contactless credentials: HID iClass, HID iClass SE, HID iClass Seos, SIO on MIFARE Classic, SIO on MIFARE DESFire EV1, MIFARE Classic, DESfire EV1, NFC-enabled mobile phones, Bluetooth Smart-enabled mobile phones.
7. Communication between access control system and device is protected by AES 128-bit encryption via the SDK. Programmable for time zones, holidays, and automatic unlocking.
8. Power and communication from one Ethernet (CAT5e or higher) cable. Compliant with 802.3af Class 1 device specifications requiring 3.84 watts for Power over Ethernet.
9. Supports real-time system lockdown capabilities. Inside lever retracts latch bolt and deadbolt simultaneously.
10. High security mechanical key provides emergency override retraction of latch/bolt without need for electronic activation.
11. Ethernet system framework, network cabling, mounting boxes, PoE end-span/mid-span, electrical hard wiring, grounding, and connections are required for complete system functionality. All system components are by others and are specified elsewhere.
    a. Power Requirement: PoE Class 2, maximum 7 watts.
    b. Network Cabling Requirements: Cat5e or higher meeting or exceeding ANSI/TIA/EIA-568-C. 24 AWG Plenum rated.
    c. Bonding and Grounding: Meet or exceed TIA-607-B Requirements. Connect device ground cable to building electrical earth ground.

d. Network Surface Mount Box: Meet or exceed ANSI/TIA/EIA-568-C Requirements. Cat5e or higher (RJ45).

12. Acceptable Manufacturers:

a. Corbin Russwin Hardware (RU) - IN220 Series. Mortise locks - IN220-ML20234 B OA BIP NSA M17 CT6R 626 Exit Devices - ED5200N IN220 N9134 B OA BIP M110 CT6R 630 Fire-Rated Exit Devices - ED5200AN IN220 N9134 B OA BIP M110 CT6R630

B. Credential - Card, Proximity, i-Class HID SEOS (shall be bend resistant).

C. Door Position Sensor - Shall be an integrated component of the Assa Abloy lockset.

D. Request-to-Exit Sensor - Shall be an integrated component of the Assa Abloy lockset or the Assa Abloy (Corbin Russwin) panic/exit device if the door is so equipped.

E. Exit Hardware - Shall be an integrated component of the Assa Abloy lockset, or a separate device as manufactured by Assa Abloy (Corbin Russwin).

F. Power Supplies for Door Locking Hardware - Shall be as manufactured by Altronix.

G. IP Compatible Door Controller - Shall be as manufactured/specified by Imron.

2.05 PACS HEADEND/SOFTWARE BASIS OF DESIGN TECHNICAL PERFORMANCE SPECIFICATIONS

A. The System shall be used to provide scalable access control, alarm monitoring, video integration, photo identification badging, and security control functions within the user's facility or facilities as specified.

B. The System shall be supplied using "standard" English text, however other languages shall be supported - these shall include but not be limited to: French, Portuguese, Spanish, Italian, German, Arabic, Finnish, Swedish, and Chinese.

C. Additionally, a flat file will be available that will allow a trained Dealer/Integrator to customize the language subset to meet local or regional preferences. The language choice will be operator specific; thus, an operator logging in on one workstation, shall by password choice, automatically be selected the appropriate language preference of their choice for that workstation.

D. The Security Management Software shall consist of the following basic components:

1. Field Hardware: Field panels, as defined herein, shall be used to support access control, alarm monitoring, video management and facility control (relay output control) functions within the defined facility or facilities as specified. An Intelligent System Controller shall serve as a distributed database management controller which shall connect to card readers, monitor point inputs, and system outputs. The intelligent controller(s) shall support on-board access readers and control terminations allowing the controller and readers to be managed with local on-board operational intelligence.

2. Field panels, as defined herein, shall be used to support access control, alarm monitoring, video management and facility control (relay output control) functions within the defined facility or facilities as specified.

3. IP-Centric Intelligent Controller, as defined herein, shall be used to support access control, video management utilizing IP-based cameras and facility control (relay output control) functions within the defined facility or facilities as specified. IP-Centric Intelligent Controller shall support multi-class credential technology utilizing the same footprint as a traditional reader. These readers shall communicate to the controller via

either Wiegand or RS485 communications protocol. The IP-Centric Intelligent Controller shall provide a complete and full-featured access control hardware and software infrastructure utilizing contactless smart card capability. IP-Centric Intelligent Controllers shall provide a complete and fully featured hardware and firmware infrastructure for access control systems with the option to communicate without host software or a dedicated server via industry standard TCP/IP protocol, over 10/100 Mbps Ethernet or the Internet. Existing Ethernet cabling can be used to power said controller utilizing 802.3af POE Specifications. IP-Centric Intelligent Controller shall provide up to 500ma shared power between lock and reader. IP-Centric Intelligent Controller shall not require sub controllers to provide distributed intelligence for up to one access point, including I/O portal management and supervision. IP-Centric Intelligent Controllers shall contain on-board flash memory allowing program updates to be downloaded via the network. Said controller shall be a UL 294 listed component and Plenum rated.

4. SMS Host Computer: The SMS host computer shall be a personal computer (PC) running the SMS application (server) software. The SMS host computer shall provide centralized security control, alarm and event monitoring and response, as well as database configuration and management for all Intelligent Controllers and associated sub-controllers within the user's facility or facilities as specified. SMS software applications that do not support multiple hardware platforms to include but not be limited to the following: Mercury, HID VertX and Edge, ACP/InBio, AXIS, Allegion, ASSA ABLOY, access control hardware platforms and Bosch B and G series, ELK M1, DMP 500/550, Alarm Control Panels, AXIS Camera Station, AXIS A8004 Video/intercom, Milestone Video Management Systems simultaneously shall be viewed as Non-Compliant.
5. SMS Operator Workstations: The SMS Operator Workstations shall be a Personal Computers (PC) running SMS application client software. The Server and Operator Workstations shall serve as the main user interface to the System and shall be used for programming, administration, and monitoring functions. Operator Workstations shall use concurrent licensing and requires one license for each initiated client; said licensing shall pertain to both thick and thin client licenses.
6. SMS Thin Client shall have an integrated webserver not utilizing such applications as IIS (Internet Information Server), Apache, or PHP. SMS Thin Client shall be browser and OS (Operating System) agnostic with capabilities of running said application on PDAs and web-enabled devices. The SMS Thin Client shall include 128bit SSL encryption. The Server and Thin Client shall serve as the user interface to the System and shall be used for programming, administration, and monitoring functions. Thin Clients shall use concurrent licensing and requires one license for each initiated client; said licensing shall pertain to both thick and thin client licenses. No separate application software shall be required for SMS Thin Client support. Any systems requiring a separate app shall be considered as non-compliant. The SMS shall be able to support up to 1000 separate thin client users.

2.06 SYSTEM ARCHITECTURE

A. The System shall make use of flexible 'Open Hardware Protocol' architecture as well as having an 'Open Database Connectivity' (ODBC) compliant System design that facilitates the sharing of data with external databases and the integration of a wide range of security

hardware, including simultaneous implementation of Mercury, HID VertX and Edge, ACP/InBio, AXIS, Allegion, ASSA ABLOY, access control hardware platforms and Bosch B and G series, ELK M1, DMP 500/550, Alarm Control Panels, AXIS Camera Station, AXIS A8004 Video/intercom, Milestone Video Management Systems simultaneously shall be viewed as Non-Compliant.

B. The System shall use 'industry-standard' hardware and state-of-the-art operating Systems. The System software shall utilize 'industry-standard' application software for System functions such as databases, graphical user interfaces, and communications.

C. Systems which use 'proprietary' computer hardware, operating Systems, field hardware or databases shall be viewed as Non-Compliant.

D. The operating System for the SMS shall maintain a current Windows Operating System Platform including all Windows Updates and hot fixes. All SMS client and server software shall have been written as native Windows applications. Systems which use an underlying operating System other than the Windows OS products (such as VMS, LINUX or UNIX) shall be viewed as Non-Compliant.

E. The SMS shall make use of such databases as Microsoft Access, MSDE, Microsoft SQL Express, and Microsoft SQL Server. Said database shall make use of an 'Open Database Connectivity' (ODBC) compliant System design that facilitates the sharing of data with external databases and the integration of a wide range of security hardware.

F. The SMS shall have the ability to import and export personnel information based on time schedules, TCP commands, and file date/time modification. The SMS System shall have the ability to import access control data including personnel, hardware, and time schedules to be used for System takeovers. The SMS System shall have the ability to import using an 'Open Database Connectivity' (ODBC), Text, Active Directory and/or CSV file. All Systems without this capability shall be viewed as Non-Compliant.

G. The SMS shall use a single hardware key 'dongle' at the server to define System configuration. The dongle shall be transferable from one server to another if a computer failure occurs. The System configuration on the dongle shall facilitate an easy System retrofit or service by the user if required. The SMS System shall allow for use of a registration key in lieu of a dongle if required. No other type of hardware key shall be required in the System. System software keys provided by the manufacturer or bidder which is not fully in control of the user shall be viewed as Non-Compliant.

2.07 USER INTERFACE - GENERAL

A. The SMS shall be designed for use by non-technical personnel who have been assigned responsibility by the end-user for managing the System. For the purposes of this document, the term System Operator shall mean any person or employee who has responsibility for managing or operating the Security Management Software, or any portion thereof.

B. The System shall provide a hardware "wizard" tool that shall intuitively guide the dealer/ integrator through the process of setting up field hardware. This shall minimize the additional technical support Requirements that traditional SMS's have required to set up the system.

C. System shall allow authorized System Operators or Trusted Agent to define and modify System operating parameters, such as cardholder records, doors, time codes, monitor points, alarm conditions, and the like. For the purposes of this document, the term Trusted Agent shall mean any person cleared by the facility for such purposes as installation,

configuration and maintenance of said SMS System. For the purposes of this document the term configuration shall mean the definition of System operating parameters and defining System hardware by a System Operator and/or Trusted Agent.

D. The System 'client' software shall allow 'industry-standard' computers to serve as 'workstations' for the Security Management Software. For the purposes of this document, the term 'Operator Workstation' shall mean an industry-standard computer running client software and serving as a workstation for the Security Management Software.

E. The 'Thin Client' shall be browser agnostic allowing any web-enabled hardware device to serve as the interface for the SMS. It shall not require a separate app be purchased to run the browser based remote login process.

F. Operators Workstations shall be connected to the SMS host computer using TCP/IP Ethernet protocol and fully function within the end-user's Ethernet network.

G. The use of a personal computer as an Operator Workstation shall not prevent other application software such as word processors, spreadsheets, and electronic mail programs from being used on the same computer.

H. The System shall be multi-user, multi-tasking, allowing the simultaneous use of multiple Operator Workstations. The System shall allow any number of Operator Workstations to be in use at the same time.

I. The System shall additionally support multi-lingual access via workstations such that the unique log on credentials may define the language of choice they may use to interact with the system.

J. The System software provided shall be capable of operating using different database management applications. Acceptable database management applications are 'Access' or 'SQL'.

2.08 USER INTERFACE - GRAPHICAL FEATURES

A. The System application software shall provide the operating features indicated herein. System software shall use menu-driven commands and provide interactive prompts. System shall use English language program and error messages, providing clear and understandable sequences of events. The user interface and menu structures shall be consistent throughout the System. The System shall have multi-language support for error messages and menu items.

B. System shall provide a standard Windows-style graphical user interface that makes extensive use of graphical elements such as toolbars, icons, and pull-down list boxes. System commands and functions shall be available by using a 'mouse' type pointing device. Text- based Systems which require the entry of commands on a command line shall be viewed as Non-Compliant.

C. The System shall use the Microsoft Windows graphical user interface and shall have the 'look and feel' of a standard Windows application program. System shall comply with established standards and conventions set forth for Microsoft Windows applications, including the ability to drag and drop items, such as access levels and graphical maps.

D. All System functions shall be available through the use of the graphical user interface. It shall not be necessary to 'shell-out' of the graphical user interface to execute any System command. It shall be possible to access the System control panel from within the application and return to the application without minimizing any active System windows.

E. The System shall offer the ability to add custom command buttons allowing the operator to click on the button to execute commands. Said command buttons must have the capability of being password protected. Up to 50 command buttons shall be available to the operator. The command buttons must have the capability of being partitioned by profile allowing only those profiles designated to view and control the command buttons.

2.09 USER INTERFACE - OPERATOR RESTRICTIONS

A. Access to any SMS Workstation/Thin Client shall require an Operator username and password. The System shall default allowing a minimum of 50 individual operator files. The number of operator files shall be user defined. Operator files shall be shown in a drop-down window display box. Adding an operator shall require an operator profile, an operator name, an operator password and/or an access credential or token. The use of a credential or token shall be user selected. Operator passwords shall be stored in encrypted form and shall be hidden except from the highest-level System Operator. The SMS shall allow use of strong passwords which includes uppercase and lowercase letters as well as numerals within passwords. System should include the ability to utilize either SMS System Authentication or Windows Authentication with the ability to integrate to LDAP

B. System shall provide multiple System Operator password profiles, each allowing a different degree of System Operator privilege, as configured by the user. Adding a profile shall require an operator name, an operator password and/or an access credential or token. The SMS shall provide no less than fifty User IDs with the ability to assign unique passwords and operator roles as a default. The total number of operator profiles shall be user defined. An operator profile shall allow various groupings of commands and System functions to allow access to those System commands and functions as determined by their password profiles.

C. Password profiles shall require the following data entered for each operator as a minimum:

1. General:
    a. Profile Name
    b. Start-up Display Screen
    c. Language
    d. Auto Alarm Call up
    e. Alarm Manager Administration
2. Options:
    a. Log-on - Password, (Password required to Log-on)
    b. Log-off - Password, (Password required to Log-off)
3. Controller Groups: This feature will allow an administrator to assign or deny access by an operator to any System Controller Group. System shall include the ability to conceal such items as System messaging, personnel records, access levels and hardware utilizing System Controller Groups.
4. Properties: Each application module shall allow administrative selection for operator access, view, add, change, delete and commands. At a minimum the administrator shall have the ability to set operator profile conditional access for the following System functions: Access Control, Access Levels; Time Schedules, Device Groups/Areas, Point Status monitoring and commands, Event Management, Alarm Management, Conditional

Commands (triggers and macros), Custom Commands, Video Management, Graphics, System Settings, System Utilities; Personnel Information including the ability to assign field level permissions of: No Access, Read/Write, Read Only, Mask Field.

D. All System functions shall be available at any Operator Workstation provided that the System Operator has the correct role. The System shall not require that System functions be segregated by workstation, i.e., there should be no distinction between a 'System administration workstation', 'alarm monitoring workstation' or 'badging workstation' once configured. Any system requiring separate workstations for different "classes of users" shall be considered Non-compliant.

2.10 USER INTERFACE — HELP

The System shall have a complementary support site that is accessible on the internet. The support site should have technical information, System instruction and troubleshooting information. This site should not require a user login and should be available in multiple languages.

2.11 ACCESS CONTROL FEATURES

A. The System shall provide card access control of doors, gates, elevators, and other portal control locations as defined herein.

B. All card readers in the System shall read the credential information programmed in access cards presented to a reader and pass verified information through an intelligent control processor for authorization. The intelligent controller shall maintain all card information locally and verify reader information received against stored System Operator-specified criteria. If a card's programmed information meets the stored criteria in the intelligent controller, then a return signal will be sent to unlock the electrically controlled door and initiate an 'Access Granted' condition message to the central System for operator notice. Using local on-board reader terminations will allow programmed information to manage access without the need for sub-controller (SC) modules. If card information does not meet System Operator-specified criteria, the intelligent controller shall initiate an 'Access Denied' alarm condition message including a descriptive event message detailing reason for the 'Access Denied' condition to the central System for operator response. The descriptive 'Access Denied' event message may include but is not limited to 'Access Denied: Level', 'Access Denied: Time', 'Access Denied: Card'.

C. Each access portal shall be provided with a card reader and directly linked to an intelligent controller module interface with on-board reader port(s). Each intelligent controller shall provide a contact output for each card reader used to unlock electric door locks and/or other devices. The Output from an intelligent controller module interface with on-board reader port(s) shall provide a normally open and normally-closed contact configuration. Output time shall be operator-definable and capable of being adjusted from 1 to a minimum of 60 seconds for each access output. The combination of card reader and output shall be defined as a 'Door' or 'Portal'. The System software shall be designed to support a minimum of two doors with expansion to two thousand and forty-eight (2,048) Doors with no change to the user interface or Requirement for retraining operators. Systems that require re-training when expanded or change the basic System GUI shall be viewed as Non-Compliant.

D. The SMS System shall include door held and door forced conditions with configurable door held times up to 2048 seconds. The SMS System shall be configurable to allow for masking

of door forced and door held conditions. The SMS System shall include the ability to configure an unlimited access grant time to be used in conjunction with Extended Grant Time Settings (American Disability Act mode). The Extended Grant Time Settings shall be configurable per portal or reader.

E. The SMS System shall include the ability to configure a door de-bounce time up to 15 seconds. The SMS System shall contain the ability to assign up to eight (8) door reader modes including: disabled, unlocked, locked (no access, allow REX), correct facility code required, card only, pin only, card and pin, or card or pin.

F. The SMS System shall include the ability to configure the offline reader modes to include: no offline mode, locked down (no access, no REX), unlocked, no access allow REX, or correct facility code mode only.

G. The SMS System shall include the ability to configure video links allowing live video to be displayed upon access or event for an individual portal or reader. The SMS System shall allow for customizable alarm messages to annunciate on a pre-defined alarm condition. The SMS System shall allow for customizable alarm multimedia files on a pre-defined alarm condition. The SMS System shall allow for configurable maximum cardholders per intelligent controller and shall also allow for configurable maximum events per intelligent lock and or controller.

H. The SMS System shall include the ability to view and configure all drivers, intelligent controllers, devices, readers from a hierarchical tree structure with a uniquely assigned addressing schema. The SMS System shall contain the ability to view real-time status and date/time of the intelligent controller and "smart" locks. The SMS System shall contain the ability to view real-time status of inputs, outputs and reader modes. The SMS System shall have a viewable loaded card count on a per controller basis. The SMS shall have the ability to control hardware devices from the hierarchical tree with unique hardware addressing down to the device level. The SMS System shall have the ability to sort the hierarchical tree alphabetically or numerically, the sort order shall follow the hardware properties throughout the software.

I. The System shall provide the capability for an authorized operator to assign an alphanumeric description (name) to each hardware hierarchical device. Descriptive name fields shall allow for a minimum of fifty alphanumeric characters. The Descriptive name fields shall be used on System menus, displays and reports.

J. The SMS System shall support up to 255 regionalized access levels per controller group with up to 1000 controller groups per server. The SMS System shall support the ability to assign alphanumeric characters to each access level. The Access Level name shall allow a minimum of fifty alphanumeric characters. The SMS System shall allow for Access Control Reader Groups or individual readers to be added to access levels using a drag and drop method or selection by menu. The SMS System shall allow for pre-defined time schedules to be associated with an individual reader or access control reader group. The SMS System shall allow for a reader or access control reader group to be added to more than one access level with a different time schedule.

K. The SMS System shall support 'Access Control Reader Groups'. An Access Control Reader Group shall be an operator specified combination of one or more portals or doors associated to a time schedule. The SMS System shall allow the assignment of portals or doors to the Access Control Reader Groups with a drag and drop function or maybe added from a menu

selection. The System shall allow an operator to define Access Control Reader Groups as required without limiting System expansion.

L. The SMS System shall support 'Elevator Assigned Floor Groups'. Elevator Assigned Floor Groups shall be an operator specified combination of one or more portals or readers associated to an access level and time schedule that have been pre-defined with an elevator assignment. The use of Elevator Control shall not require the purchase of an additional option but shall be standard any SMS systems requiring the purchase of additional software to support Elevator control shall be considered Non-compliant.

M. The System shall provide the capability for an operator to assign an alphanumeric name to each Access Control Reader Group. Access Group name shall allow for a minimum of fifty alphanumeric characters. The Access Group name shall be used on System menus, displays and reports.

2.12 ANTIPASSBACK FEATURE

A. The SMS System may be a system where card readers are used for both entrance and egress. In this event the system shall allow each card reader to be operator-defined as either an 'entry or 'exit reader'. The System shall require cardholders using a card at an 'entry' reader to subsequently use the card at an 'exit' reader before the card can once again be used at an 'entry' reader, creating an Anti-Passback condition. Cardholders attempting to use cards without first exiting the Anti-Passback area shall be denied access and shall cause a 'Passback Violation' message to be sent to the central System for operator notice. If so configured, Passback Violations shall create an Alarm Condition causing an immediate report generated for operator alarm response.

B. The System shall provide a Passback 'forgive' feature that can be activated by an authorized operator. The Passback forgive feature shall reset the Passback status of any card to a neutral condition (neither 'in' or 'out' of the anti-Passback area), allowing the Passback sequence to be restarted.

C. The System shall allow the Anti-Passback feature to be enabled and disabled upon authorized operator command,

D. The System shall allow the APB mode to automatically be "reset" by a Time Code without the need to use an "exit" reader.

E. A special Anti-Passback set flag shall be provided in the access control personnel record file that allows and authorized operator to specify a cardholder as Anti-Passback exempt. If a cardholder has the Anti-Passback exempt flag set they may enter or egress any Anti-Passback area without causing an Anti-Passback event or alarm.

2.13 ELEVATOR CONTROL FEATURE

A. The System shall support elevator access control based on user Controller Group Requirements and configuration. The actual number of cars and floor selection outputs shall be user configurable. The System shall provide for the following elevator access control features, elevator call, and elevator floor select for individual or a group of elevator cars:

1. Elevator call shall be an operator command or a time scheduled condition that electronically bypasses the normal use of an elevator call button at secured or unsecured floors.

2. During a command or time scheduled event the normal elevator call button conditioning shall be replaced with an access reader-controlled output. If any cardholder presenting his or her card to such a reader is authorized a sub-controller output shall activate the elevator call button to that floor.

B. Elevator floor select shall be an operator specific configuration of card readers and outputs designed to allow authorized cardholders to enter an elevator and access only floors they have been pre-defined to access by a System operator. Elevator floor access selection replaces the normal elevator select push buttons inside the elevator car. To operate an access elevator car, a cardholder must present his or her access card to a card reader located inside the elevator car. The System shall respond to a valid access by activating outputs which temporarily enable the floor selection buttons for those floors to which the cardholder is authorized. The System shall allow outputs from elevator car floor selection buttons to be connected as monitor point inputs to the System to identify which floor was actually selected by each cardholder. Once a floor is selected the system shall automatically reset allowing another authorized cardholder to select another floor. The elevator control feature shall provide a fully distributed functionality allowing managing access requests and activating floor selections even when an Intelligent Controllers is 'off-line' with the SMS host computer. The System shall not rely on the SMS host computer to provide elevator control functions. Systems that use a separate central computer for elevator control decisions shall be viewed as Non-Compliant.

2.14 DEFINITION OF ACCESS PRIVILEGES

A. The System shall use a flexible, modular method of defining 'who', 'where' and 'when' a cardholder will be authorized access or egress secured locations within a defined site.

B. As a cardholder is entered into the database the System shall automatically build a record and allow an authorized operator to assign access privileges. 'Who' shall be defined as the System defined cardholder.

C. Assigning an 'Access Level' to a cardholder record defines 'where' that cardholder will have access within the facility or facilities.

D. The SMS data base shall support up to 10 unique ID's (cards) per cardholder that may be assigned for other offsite facilities or assets assigned to an individual cardholder.

E. The System shall allow multiple Access Levels consisting of a combination of Access Control Reader Groups, Temporary Access levels and General Access levels. The System shall allow for Time Schedules to be configured by Access Control Reader group.

F. The System shall allow for an automatic Temporary Access start and stop date to be configured.

G. Assigning a 'Time Schedule' to readers and cardholders defines 'when' a cardholder will have access within the facility or facilities.

H. A Time Schedule shall be operator-specified combinations of Time Intervals and Days of the Week used to specify times that a card may be used to gain access throughout a facility or facilities. Each Time Schedule shall allow not less than twelve individual Time Intervals for each day of week Holidays shall have multiple Time Intervals scheduled as well. The System shall allow for Holiday Time Schedule overrides by time schedule and interval.

I. Cardholder records, Access Levels and Time Schedules shall be definable by authorized System operators. To configure a Time Schedule the user shall select days of the week and

hours of the day that will make up each Time Schedule. Time Schedules shall also have 'Time Interval'. A 'Time Interval' shall be defined as a range of times that can be contained within a 24-hour day. (An example of a Time Interval would be: 00:00 - 22:00 and 22:15 - 23:59/12:00 AM - 10:00 PM and 10:15P M - Mid-night). Time intervals shall maintain a precision of 1-minute (60 seconds) or less. The System shall allow an authorized operator to define as many Time Intervals as required by the installation with a minimum of twelve 'Time Intervals' per day for the AXIS. Time Intervals shall have the ability to be changed using a drag and drop graphic or by typing in the numeric time value.

J. A 'Holiday' shall be an operator-specified date treated by the System as a Holiday. On dates defined as a Holiday, the System shall use the time criteria specified for Holidays by a System operator. The System shall allow a System operator to specify Holidays as required by the site. The System shall provide for up to 8 holidays per time schedule. Systems that do not support eight holidays per time schedule shall be viewed as Non-Compliant.

K. The System shall allow an authorized operator to assign an alphanumeric name to each Access Level, Time Schedule and Holiday. These names shall allow for a minimum of fifty alphanumeric characters. These names shall be used on System menus and reports.

L. The System shall allow an operator to establish an 'Activation Date' for each cardholder/card. The Activation Date shall be the date that access privileges associated with that cardholder/ card shall take effect.

M. Cardholders attempting to use an access card before the Effective Date shall cause an Invalid Access Attempt condition message at the central System for operator response.

N. System shall allow the System Operator to establish a 'Deactivation Date' for each cardholder / card.

O. The Deactivation Date shall be the date that access privileges associated with that cardholder / card shall be canceled. Cardholders attempting to use an access card after the Expiration Date shall cause an Invalid Access Attempt message at the central System for operator response.

P. The System shall support vacation start and stop dates to temporarily deactivate a cardholder card while they are listed as being on vacation and away from their normal work area. Systems that do not have and automated vacation set shall be viewed as Non-Compliant.

Q. The System shall support a temporary access level assignment selection with automated start and stop dates. This allows an administrator or authorized operator to assign additional access rights to an individual for a specific number of day and automatically cancel the exception. Systems that do not have an automated temporary access level assignment set shall be viewed as Non-Compliant.

R. The System shall allow for the automatic deactivation of cardholder records if the card has not been used within the designated "Days of Non-Use before Card Deactivation" value. This value shall be configurable by the System Operator. This feature shall have the ability to be disabled if the System Operator so decides.

2.15 CARDHOLDER RECORDS

A. The System shall provide a unique 'Cardholder Record' to store data for each cardholder in the System. The System shall provide capacity for as many records as required by the operator.

B. The System shall provide a four-tab data entry screen (form) allowing the creation, editing and deleting of Cardholder Records. The Cardholder Record shall contain the following fields and functions as a minimum:

1. The System shall display the following form control using graphical icons:
    a. Lock: Shall be used to LOCK / UNLOCK records for operator editing.
    b. Plus: Shall be used to ADD a new card record or to make a COPY of an existing card record.
    c. Disk: Shall be used to SAVE a record or data entered.
2. X: Shall be used to DELETE a record.
    a. Binoculars: Shall be used to FIND records and filtered database lookups.
    b. Drum: Shall be used to do GROUP EDITS. The System shall allow editing of all personnel fields using group edits. The System shall allow for Card Templates to be created allowing for predefined values to be assigned automatically to any card record assigned the Card Template. The Card Templates shall have permissions assigned by profile. The Card Templates shall automatically update any records with any values modified in the Card Template.
    c. Drum Arrow: Shall be used to DOWNLOAD all or selected database changes to the effected Controllers.
3. Tab One - Access Control / Employee Info:
4. Card Record Count: The System shall display a filtered and actual card record count allowing an operator to move up and down records using an ascending and descending slide.
5. First Name: Shall show 1 to 30 alphanumeric characters, first name field.
6. Initial Field: Shall show 1 alphanumeric character, initial field.
7. Last Name: Shall show 1 to 30 alphanumeric characters, last name field.
8. Card Type: Defined card types. The System shall support pre-defined data entry forms. This feature shall allow the operator to pre-define data fields reducing error and data entry time.
9. Cardholder Identification Number: 1 to 12-digit record number. Cardholder number entry shall support an automated reader number entry or manual number entry.
10. Card Hot stamp number: Shall show 1 to 12 numbers only.
11. Card Re-Issue Code: Last card issued count. The System shall support a card issue count for each card re-issued to a cardholder.
12. PIN Number: Shall show 1 to 8 digits' user defined Personal Identification Number, if used.
13. Cardholder Name: 1 to 30-character alphanumeric name.
14. Access Card Number #1 - #10: Shall support 12 digits or more access card number sen-coded on the cardholder's primary access card.
15. Trigger Code: Shall display the code association for cardholder trigger/macro conditioning.
16. Activation Date: Shall show the date when access privileges are to begin.

17. De-activation Date: Shall show the date when access privileges are to expire.
18. Company: Company Name shall use a drop-down window 1 to 48 alphanumeric characters.
19. Department: Department Name shall use a drop-down window 1 to 48-character alphanumeric characters.
20. Title: Job description. 1 to 50 alphanumeric characters.
21. Social Security#: Employee Social Security Number (xxx-xx-xxxx) numeric only.
22. Employee#: Company employee number 1 to 20 alphanumeric characters.
23. Email Address: 1 to 40 alphanumeric characters.
24. Access Levels Tree: Show all Controller Groups, access levels and groups associated with the cardholder record.
25. Date of Birth: The System shall provide a right-click calendar display to select date.
26. Date of Hire: The System shall provide a right-click calendar display to select date.
27. Work#: 15 telephone alphanumeric characters
28. Home#: 15 telephone alphanumeric characters
29. Address-1, 2: 2 lines 50 alpha-numeric characters each for address information.
30. Last Modified: Shall be used to show last modification data and log-on operator.
31. Last Print: Shall be used to show the last date the record was printed by an operator.
32. Tab Two - Custom Fields:
33. Custom Fields: Provide up to 20 data fields, 1 to 50 alphanumeric characters each. The System shall allow for a date / time stamped notes table for general data entry.
34. Tab Three - Advanced Access Control:
35. Vacation Start Date: The System shall provide a right-click calendar display to select date. Cardholder card shall be suspended from access on this date.
36. Vacation Stop Date: The System shall provide a right-click calendar display to select date. Cardholder card shall be re-activated for access on this date.
37. Temporary Access Level Start Date: The System shall provide a right-click calendar display to select date. Cardholder shall be assigned the temporary access level on this date.
38. Temporary Access Level Stop Date: The System shall provide a right-click calendar display to select date. Cardholder's temporary access shall be removed on this date.
39. Card Use Limit: This shall define the number of times the card may be used for access.
40. Guard Tour Flag: Shall be used to identify the card as a guard tour card.
41. Activate Card Flag: Shall be used to suspend a card by an operator without deleting the cardholder record.
42. Free Anti-Passback Flag: Shall be used to allow a card access or egress in an anti-Passback area without activating an operator notice.
43. Anti-Passback Exempt Flag: Shall be used to allow free access or egress in any anti-Passback area without activating an operator notice.

44. A.D.A Flag: Shall be used to set momentary time for ADA persons, extending door lock and held open timers.
45. PIN Exempt Flag: Shall be used to set all cardholder reader access to card only.
46. Alter Current Anti-Passback Location Flag: Shall be used to hold a current anti-Passback status for a cardholder when access is granted.
47. Alter Current Use Count Flag: Shall be used to hold a current use count on a specific area when access is granted.
48. Reset Anti-Passback Flag: Shall be used to reset a cardholder Anti-Passback status.
49. Access Trace Flag: Shall report the last fifty card presentations and shall display the date and time the card was presented; the location of the presentation including the physical address and description and shall display the associated detailed event.
50. Tab Four - Photo ID Badging:
51. Badge Window: Shall display user defined badge format.
52. Capture Device: Shall allow an operator to select multiple types of cameras or board capture devices.
53. Live Video Icon: Shall allow an operator to select a live video view through the capture camera.
54. Video Configuration Icon: Shall allow the operator to define properties for video format, video display and video source.
55. Twain Devices Icon: Shall allow the operator to select installed TWAIN devices for digital capture.
56. Acquire from TWAIN: Shall allow the operator to collect a stored or newly acquired digital image.
57. Save Photo Icon: Shall allow the operator to store an image in the cardholder record.
58. File Open Icon: Shall allow the operator to save a stored image into the cardholder record.
59. Clear Photo Icon: Shall allow the operator to clear a photo from the cardholder card production viewer.
60. Crop Size Icon: Shall allow the operator to crop a photo to fit a specific badge frame size and show the best view of the image.
61. Capture Signature Icon: Shall allow the operator to display, save and print a signature on a card when equipped with a signature reader.
62. Badge Template Box: Shall allow the operator to select a badge template for the cardholder record.
63. Preview Badge Icon: Shall allow the operator to view a printable badge.
64. Edit Badge Layout Icon: Shall allow the operator to view and edit a selected badge template.
65. The Badging System shall allow for batch printing of cards.

2.16 CARDHOLDER RECORDS (PART 2)

A. The System shall use the Cardholder Identification Number as the primary key to uniquely identify the record in the database. The System shall permit the use of access card numbers as a key but shall not use access card numbers as the primary key unless defined by an operator.

B. The System shall provide a sort-list of card holders per Controller Group selected on the Personnel Manager screen. Sort-keys shall allow the list to be sorted and displayed for an operator.

C. The System shall permit the use of access cards encoded in Wiegand formats of varying bit lengths from 26 bit to 75 bit

D. Note: Card bit format limitations and constraints are controlled by the field hardware. It shall be the responsibility of the bidder to ensure that the field hardware proposed can meet the Standards as set forth in the Specification/RFQ.

E. The System shall allow not less than ten different access card numbers to be assigned to each cardholder record. The System shall not require that a separate cardholder record be created for each access card number. The System shall allow each access card number on the card-holder record to use a separate format. Systems that do not support a minimum of ten cards per cardholder record shall be viewed as Non-Compliant.

F. The System shall permit the creation of a Cardholder Record without requiring that an access card number be assigned. This feature shall allow a Cardholder Record to be created for "PIN Only' users who will be assigned a PIN number (1 to 8 digits) only and not an access card.

G. The System shall provide a hierarchical tree showing access level assignment for each card-holder in the Cardholder Record. This tree shall permit an authorized operator to list, and select, through 'pop-up and drop-down windows', any access level or access group defined in the System. To view access levels and access group shall not require an operator exit from the Cardholder Record screen to perform this function.

H. The System shall allow the System Operator to identify the Access Levels, Access Groups, readers and Time Schedules associated with each cardholder without requiring the System Operator to exit from the Personnel Manager screen.

I. The System shall allow for the automatic disabling of card records based on the configured "Days of Non-use before Deactivation" value.

J. The System shall allow for the Personnel Manager heading tags to be modified to reflect headings based on the customer's request.

2.17 AUTOMATIC ADJUSTMENT FOR DAYLIGHT SAVINGS TIME

The System shall provide an ability to automatically adjust the System time to accommodate changes at the beginning and end of Daylight Savings Time. System shall allow the dates associated with Daylight Savings Time to be set by System Operator in advance.

2.18 PARTITIONED DATABASE FEATURE

A. The System shall provide the ability to establish multiple 'Logical Views' of the Access Control System and cardholder database. Each Controller Group shall permit viewing and/or modification of only certain cardholder record fields, access levels, access groups, hardware configuration, and other such data. This capability shall allow the creation of 'Controller Group', logical Sub Systems. The System shall allow an authorized operator to create as

many Controller Groups as required for a site or multiple sites. Systems that do not support a Controller Group management set shall be viewed as Non-Compliant.

B. Each Controller Group shall have full System capabilities; and shall appear to the System Operator and operate as if it were an independent Access Control System. The typical Controller Group may consist of a single building or multiple building; or a single department in multiple buildings, or a single department within a building which houses multiple departments.

C. Creation of Sub-Systems shall be accomplished through System Configuration and software partitioning of the database.

D. The System shall allow System Operator profiles to view, create, or edit data in only certain Controller Groups. As an example, a System Operator who is assigned an operator profile for access to Controller Group 1 shall only be able to view and edit database records affecting Region 1. This System Operator would be restricted from viewing and modifying other portions of the System database based on his or her operator profile. An operator profile shall allow the System Operator to assign one or more Regions for operator access.

E. The System shall allow the ability to partition the hardware down to the device level. The System shall allow System Operator profiles to view, create, or edit hardware data for only those devices designated to the Operators profile. Systems without the capability of partitioning hardware at the device level shall be viewed as Non-Compliant.

F. System Operator functions which may be restricted by operator profile and Controller Group shall include, but shall not be limited to, the following:

1. Adding, deleting, and modifying Cardholder records.
2. Locking and Unlocking of Doors.
3. Arming and Disarming of Secure Areas
4. Masking and Un-masking of Alarms
5. Printing Reports.
6. Configuration of Access Levels, Time Schedules, Access Groups, and other such system parameters.
7. Establishment of automatic door lock and unlock times.
8. Monitoring of Alarm Conditions from user defined Doors and Monitor Points.

G. The System shall allow the assignment of any Door, Access Group, Monitor Point, Device Groups/Areas, Auxiliary Output Contact or other System element within a Controller Group.

H. It shall be possible to assign any Door, Access Group, Monitor Point, Device Groups/Areas, Auxiliary Output Contact or other System element to more than one Region at the same time.

I. Operator access to specific Controller Groups shall be determined by System Operator username and password. The use of Controller Groups shall not prevent authorized System Operators from making System-wide changes or generating System-wide reports.

J. As an example, it shall be possible for an authorized System Operator to add/delete a cardholder from all sub-Systems with a single entry. The System shall not require that a separate entry be made to add/delete a cardholder from each Controller Group. Systems that require data add/delete entries in multiple partitions within the application shall be viewed as Non-Compliant.

2.19 INTERFACE TO EXTERNAL DATABASES

A. The System shall provide the ability to 'Import' information into the Security Management Software host computer from existing data compliant personnel databases. The purpose of importing this information is to minimize the need for persons managing the Access Control System to manually enter data. Some of the desired capabilities include:

1. The ability to import information from the databases for the initial load of the cardholder database, and for major loads of new information periodically.
2. The ability to update the cardholder database based on the import of an 'Exception File' reflecting changes in employee status.
3. Import of exception file shall allow the System to automatically add cardholder records, delete cardholder records, modify access privileges, and change other information contained in the cardholder database. The System shall allow the import of an exceptionfile based on User Requirements and existing database application capability.
4. The System shall allow said import to be scheduled by minute, hour or daily imports.
5. The System shall allow the import utility to be configured as a Windows Service.
6. The System shall allow import of data from Open Database Connectivity (ODBC), CSV or text files.
7. The System shall allow for Human Resource (HR) Integration such as PeopleSoft HCM through the available API/SDK from the HR system for bidirectional updates

B. New employee/user entered in the HR system will automatically add new record in the System thru the HR Integration

C. Updates to employee/user in HR system will automatically update changes of the record in the System thru the HR Integration

D. Deletion of employee/user in HR system will automatically disable/delete record in the System thru the HR Integration

E. The System shall not require a System restart or 'reboot' for data imports or updates to the cardholder record database to take effect — updates shall be made automatically upon receipt of data if so, configured by the user.

2.20 DOOR CONTROL FEATURES

A. System shall be capable of unlocking and re-locking Doors and Door Groups upon command from Operator Workstation. A command shall be capable of being executed by an authorized operator from pull-down menus, icons on status screens, text lines on event screens and icons on Custom Map Displays.

B. The System shall automatically disable Door Forced conditions and 'Door Open / Door Held' conditions from doors that have been unlocked by an operator command.

C. The System shall be capable of automatically unlocking and re-locking Doors and/or groups of Doors based on Time Schedule and Intervals. The System shall be capable of automatically disabling Door Forced conditions and Open-Too-Long conditions for Doors that have been unlocked by Time Schedule and Intervals.

D. The System shall provide the capability to selectively disable Doors upon command from designated Operator Workstations based on operator profile, username and password. Disabled Doors shall deny access to all cardholders.

2.21 AUXILIARY CONTROL FEATURES

A. The System shall provide 'Auxiliary Output Contacts' for auxiliary control purposes, such as the unlocking of non-card reader-controlled doors, operation of audible alarm devices, and other such functions. Auxiliary Output Contacts shall be capable of being assigned to Door Groups; and shall be capable of being operated upon command from Operator Workstations, automatically by Time Schedule and Interval and Triggers and Macros. The System shall provide a minimum capacity of 10,000 auxiliary output contacts.

B. Cardholder trigger codes in a cardholder record shall allow trigger and macro control for command activation and de-activation of auxiliary outputs based on access grant or deny activity. At a minimum, device groups/areas, macro conditions to lock and unlock locations, mask and un-mask access conditions, alarms, etc., shall be activated or de-activated based on a cardholder trigger code assignment.

C. The System shall provide the capability for the System Operator to assign an alphanumeric name to each Auxiliary Output Contact. Auxiliary Output Contact name shall be a minimum of fifty alphanumeric characters. The Auxiliary Output Contact name shall be used on System menus, displays and reports.

2.22 DOOR STATUS MONITORING

A. The System shall monitor the status of each access-controlled Door to determine if a door is open or closed. If an access-controlled door is opened without the presentation of a valid card the System shall generate a 'Door Forced' condition.

B. The System shall support an ADA (American Disabilities ACT) standard whereby a different shunt time can be set for a physically impaired person, so they can access with a longer held open/shunt time than other employees.

C. Where a card reader is provided only on the entry side of a door, the System shall allow the disabling of Door Forced monitor from the exit side of door. Disabling of Door Forced monitor shall be accomplished through the use of a request-to-exit input, defined as a 'REX'. A REX input shall be a normally open or closed dry contact input to System, allowing connection of release buttons, motion detectors and other devices.

D. If the System is so configured, operation of a REX input shall disable the Door Forced monitor for a System Operator-specified period of time, allowing exit without causing a Door Forced condition. If the System is so configured, a REX input shall also be capable of unlocking the door. One REX input shall be provided for each access-controlled door per door controller or smart reader lock.

E. System shall provide the capability to remotely disable REX features for each Door. Each REX shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon command from an operator workstation.

F. The System shall support fully supervised End-Of-Line input circuits which are software programmable by the System Operator.

G. The System shall monitor the status of each access-controlled door to determine length of time a door is open after an authorized access grant. If the door is left open longer than a

System Operator specified time period, the System shall generate a 'Door Open / Door Held' condition for operator notice.

H. The Door Open / Door Held timer shall be capable of being set for a System Operator-selected period of time between 1 to 4000 seconds. The Door Open / Door Held time period shall be individually selectable for each Door.

I. The System shall provide the capability to remotely disable the Door Open / Door Held monitoring feature for each Door. Feature shall be capable of being disabled automatically by Time Schedule, Triggers and Macros and upon a command from an Operator Workstation.

J. Door Forced and Door Open / Door Held conditions shall be immediately processed by the System based on parameters pre-configured by the System Operator. If so configured, Door Forced and Door Open / Door Held conditions shall create an Alarm Condition; causing an immediate report to be sent to a designated Operator Workstations through the System Alarm Manager for alarm acknowledgment; and causing other System Operator-specified System operations to occur.

K. The system shall support a minimum of three different states for any access control door/portal.

1. Door open
2. Door closed
3. Door closed, locked and secure

L. Any system that does not record the position of the door locking hardware shall be deemed non-compliant.

2.23 ALARM MONITORING FEATURES

A. The System shall provide monitoring of contact inputs from door switches, motion detectors, and other sensors located at field locations. Each input shall be defined as an individual 'Monitor Point'. The System shall provide the capacity for a minimum of 10,000 Monitor Points.

B. Monitor Point inputs shall utilize a supervised circuit requiring the use of an End-Of-Line (EOL) resistor circuit. The System shall allow an authorized operator to specify, through the System software, the EOL Circuit Requirements of each individual input.

C. Monitor Point inputs shall accept both normally open and normally closed dry contact input signals. Monitor Point inputs shall provide a minimum of three distinct states, including 'normal' (input is in normal or inactive condition), 'alarm' (input is in alarm or active condition), and 'trouble' (input is in fault or tamper condition).

D. Each Monitor Point shall be identified on System displays by a unique Monitor Point number. In addition, the System shall provide the capability for the System Operator to assign an alphanumeric name to each Monitor Point. Monitor Point name shall be a minimum of fifty alphanumeric characters. The Monitor Point name shall be used on System menus, displays and reports.

E. The System software shall provide an 'A Virtual Door Monitoring Feature'. The virtual door monitoring feature shall permit a REX input point to be logically associated in software with a Monitor Point and Auxiliary Output to create a 'Virtual' access door. This feature shall allow non-card reader doors to be monitored for both Door Forced and Door Open / Door Held conditions without requiring a card reader or card reader sub-controller.

F. Monitor Points shall be capable of being grouped for the purpose of alarm management. A Secured Area shall be a System Operator-specified group of Monitor Points. The System shall provide the minimum number of System Operator-definable Device Groups/Areas as required by the user.

G. The System shall provide the capability for the System Operator to assign an alphanumeric name to each Secured Area. Secured Area name shall be a minimum of fifty alphanumeric characters. The Secured Area name shall be used on System menus, displays and reports.

H. The System shall provide the capability to Arm (enable) and disarm (disable) Device Groups/ Areas by command from Operator Workstation and by Time Schedule and Interval. Arm and Disarm commands shall be capable of being executed from pull-down menus, icons on status screen, through triggers and macros and icons on Custom Map Displays.

I. The System Operator shall be able to enable a Monitor Point allowing the Monitor Point to cause an Alarm Condition for operator notice if point is activated or activates after enabling. The System Operator shall be able to disable a Monitor Point allowing the Monitor Point to activate without causing an Alarm Condition for operator notice. Monitor Points shall be capable of being armed and disarmed individually, and by Secured Area.

J. The System shall have capability to automatically Arm and Disarm Monitor Points and Device Groups/Areas by Time Schedule and Interval.

K. Triggers and Macros shall be capable of locking and unlocking any number of access-controlled Doors and Door Groups, change any number of card reader modes, enable and disable any number of Monitor Points and activate and deactivate any number of output points based upon a Monitor Point status change. Triggers and macros shall be System Operator configurable and shall use any Monitor Point status change, access condition change, keypad commands and/or cardholder trigger codes for conditions of change.

2.24 EXTERNAL CONTROL OF DEVICE GROUPS/AREAS

A. The System shall allow Device Groups/Areas to be Armed and Disarmed through the use of card readers designated as 'Arming Readers'. Presenting a valid access card to an Arming Reader shall toggle Device Groups/Areas from armed state to disarmed state and vice versa.

B. The System shall allow Device Groups/Areas to be managed for access into such areas using a 'Keypad Display Terminal'. The System shall be capable of managing up to 64 Device Groups/Areas from a single Keypad Display Terminal or up to 64 Device Groups/Areas across multiple Keypad Display Terminals.

C. Keypad Display Terminal alarm management shall support secured area Open / Close conditioning, tracking System Operator defined secured area early and late open and early and late close status for each defined area.

D. The System shall allow Device Groups/Areas to be Armed and Disarmed through the use of external hardwired controls (such as a key-operated shunt switch.) The System shall permit Monitor Points to be defined as a trigger to run a macro assigned to Arm or Disarm a Secured Area. As an example, when Monitor Point trigger / macros are activated, the Secured Area which it controls shall be disarmed. When a Monitor Point trigger / macro is normal (inactive), the Secured Area which it controls shall be armed.

E. The System shall allow Auxiliary Output Contacts to function as Secured Area status outputs. Two types of outputs shall be capable of being defined:

1. Armed Status Output: Output contact operates when Secured Area is in Armed Condition (typically used for 'armed-status' indicator lights).
2. Secure Status Output: Output contact operates when all Monitor Points assigned to Secured Area are in normal condition (typically used for 'ready-to-arm status' indicator lights).

2.25 CUSTOM MAP DISPLAYS

A. In addition to other means, the System shall be capable of displaying the status of and controlling System elements through the use of Custom Map Displays and configurable map levels and icons.

B. A 'Custom Map Display' shall be a dynamic multi-color graphic display that is generated on the System for System Operator viewing and interaction at workstations. Custom Map Displays shall be System Operator-created graphic displays that show maps, site plans, building floor plans, and other graphic representations of the user's facilities.

C. Custom Map Displays shall allow display of symbols (icons) representing Doors, Monitor Points, Auxiliary Output Contacts, Cameras and Secured Area Keypads and other such System elements to be placed on a map level adjacent to rooms, doors and other building features. Upon change of status, a color bar associated with the symbol/icon shall change color to identify a change of state on the graphic.

D. Custom Map Displays shall allow activation of operator commands such as the locking and unlocking of Doors, arming and disarming of Monitor Points and the operation of Auxiliary Output Contacts. Commands on Custom Map Displays shall be activated by clicking on symbols/icons representing a System element (devices) and then choosing a desired command from a selection window such as (lock, unlock, etc.).

E. Custom Map Displays shall be capable of being created using complex graphics shapes including lines, circles, multi-sided polygons, complex curves, filled objects, photos and the like. Custom Map Displays shall be capable of utilizing distinct colors.

F. System shall accept image files such as jpeg, wmf, bitmap and other standards created/edited by graphic software packages, such as MS Visio and AutoCAD.

G. System shall store maps as wmf files (not bitmaps) and shall allow "dynamic resizing" of map displays. "Dynamic resizing" shall allow a map image to be created and stored as a vector-based file. Once created, the image shall be capable of being "panned" and "zoomed" without loss of detail, allowing a single image to be viewed on screen at a zoomed scale.

H. System shall provide for up to 10 separate layers for plotting on any map. The user shall have the ability to select the layer and plot System device assigned icons as a separate layer on a map, graphic diagram.

I. System shall provide an unlimited number of unique Custom Map Displays.

J. System shall allow the use of Google Earth maps through the Thin Client. The Google Earth integration shall allow the operator to create 3D/4D custom floor plans using the free version of Google Sketch up.

2.26 ALARM DISPLAY FEATURES

A. Activation of Monitor Point shall be immediately processed by the System in accordance with parameters as established by the System Operator. If so configured, the activation of a Monitor Point shall create an Alarm Condition causing an immediate report to be sent to the Alarm Manager on the Operator Workstations. Any event/alarm shall be configurable in the Triggers and Macro module to cause other System specified operations to occur. The maximum time period from activation of Monitor Point until Alarm Condition is displayed on the Operator Workstation shall not exceed 5-seconds.

B. System shall be capable of displaying customizable Operator Instruction Displays. Operator Instruction Displays shall be System Operator-created text messages per alarm point or based on a typical response message from file. System shall provide a message file for every alarm setup by the System administrator or authorized operator.

C. Upon Alarm Condition, the System shall sound an audible warning configurable by the System Operator, display an alarm message on a graph map by the point that activated into an alarm condition on all operators logged on to the System with an alarm monitoring profile. Systems requiring Operator-designated Operator workstations only shall be viewed as Non-Compliant.

D. If so, configured any Alarm Condition shall automatically display a specified Custom Map display at any logged on authorized operator workstation. The symbol (icon) representing the Door Monitor Point, or other device causing the Alarm Condition shall change color or flash to identify point of alarm origination on the map display.

E. If so configured and Alarm Condition shall automatically display a specified Custom Operator Instruction with the specific Custom Map display.

F. The System shall provide real-time tracking of the actual status of each Armed Monitor Point, providing an indication of when Monitor Point is activated, and of when Monitor Point is cleared. A user selected Point Status Window shall be selectable by an operator to display the real-time status of all points, outputs and readers based on their regional operator profile.

G. Alarm Conditions shall require Operator acknowledgment. Administrator Operators shall have the ability to acknowledge all alarms simultaneously. In addition, the System shall allow Alarm Conditions to be configured as “log only” events.

H. The System shall provide a visual indication of all unacknowledged Alarm Conditions in the “Alarm Manager” window on any authorized operator workstation.

I. System shall provide an Alarm Manager to display the status of all active and user assigned alarm points for any logged-on and authorized operator at any client on the network. Systems that restrict alarm displays to only assigned operator workstations shall be viewed as Non-Compliant.

2.27 ACTIVATION OF OUTPUT CONTACTS UPON ALARMS

A. All Alarm Conditions, including Door Forced conditions and Door-Held-Open conditions, shall be capable of activating one or more Auxiliary Contact Outputs to enable operation of audible sounders, door alarm horns, and other such devices.

B. System shall permit the global relationship of Alarm Conditions to Auxiliary Output Contacts, where conditions occurring at one Intelligent Controller shall be capable of causing outputs to occur at any Intelligent Controller in the System.

C. The System shall allow System Operator to define how each output is to operate during each Alarm Condition. As a minimum, the System shall permit the following operating conditions all configured in a separate software module, Triggers and Macros. Systems that do not support fully configurable Triggers and Macros based on any System event/alarm shall be viewed as Non-Compliant.

1. Output tracks Alarm Condition/Event/Activity: Output activates when Alarm Condition is active and deactivates when Alarm Condition clears.
2. Output tracks acknowledgment: Output activates when Alarm Condition is active and deactivates when Alarm Condition is acknowledged by System Operator, even if Alarm Condition has not yet cleared.
3. Timed output: Output activates when Alarm Condition is active, and deactivates when Alarm Condition has cleared, or after a preset time period, whichever occurs first. Time shall be definable by System Operator for periods of between 1 and 300 seconds.
4. Access Events: Output activates or de-activates based on any access event/status change with time of day and other event conditioning.
5. Cardholder Event: Output activates or de-activates based on a cardholder trigger code and access event (granted or denied).

2.28 EMAIL OR TEXT MESSAGING UPON ALARM CONDITION

A. System shall provide ability to send E-mail messages to designated recipients upon Alarm Conditions or operator selection. System shall utilize standard SMTP E-mail protocols to permit transmission to any valid Internet Email address. This capability shall allow transmission of alarm messages to any device capable of receiving E-mail messages (pager, cell phone with text messaging, etc.).

B. Email messages shall be capable of being sent to E-mail Address Groups based on Time Code.

2.29 SOUND EFFECTS UPON ALARM CONDITION

System shall provide ability to automatically play audio messages on designated Operator Work-stations upon Alarm Condition. System shall allow attachment of separate audio and media files to each Alarm Condition. Audio files shall be standard .WAV format audio files, media files are MS Standard.

2.30 TRACE FEATURE

A. System shall provide a special Trace feature that can be set individually for each cardholder. The Trace feature shall allow special real-time tracking of System Operator-specified cards. Use of a card that has been set for Trace shall be automatically logged, and if so configured, shall cause a special report to be displayed at Operator Workstation. Trace reports are special and are in addition to any regular report as the result of card activity, such as Valid Access or Invalid Access Attempt.

B. An automatic cardholder activity report and reader access report shall be standard selection in the cardholder file. Reader access reports shall be selected from the Event Manager and display, cardholder file and graphic map icons.

2.31 SYSTEM REPORTING AND LOGGING FEATURES:

A. The System shall provide an electronic log of events, recorded on a real-time basis as they occur. Events shall be recorded with date and time.

B. When Intelligent Controllers are in an 'on-line (in communication with SMS host computer) status condition, System events shall be immediately sent to SMS host computer and stored on hard disk.

C. When Intelligent Controllers are in an "off-line' (not in communication to SMS host computer) status, Intelligent Controllers shall store ('buffer") System events in memory. Each Intelligent Controller shall be capable of storing a minimum of 5,000-Events in memory.

D. In addition to being stored, System events shall also have the capability to be immediately displayed at designated Operator Workstations, and at designated printers, providing real-time reporting of all System events.

E. The System shall support standard network printing facilities to allow the use of any printer connected to the user's local computer or network. The use of specific printers for specific types of reports shall not be required.

F. The System shall allow events to be selectively reported to Operator Workstations and Printers. As a minimum, the System shall allow the selective reporting of the following events: Alarm Condition, Monitor Point activity, Forced Door, Door-Held, Invalid Access Attempt, Passback Violation, Trace, Hardware Failure, Communication Failure, Tamper, Power Fail, etc.

G. The System shall provide the capability to generate a current System status report upon command from Operator Workstation. Status reports will indicate current status of Doors, Monitor Points, and Alarm Conditions; current status of System Operator imposed commands such as Disarm, Unlock, Disable and the like; current status of timed System operations, such as timed Unlock, timed Disarm and the like; and the current status of equipment, communications, and power failure conditions.

H. All card access activity shall be logged at a minimum. For Valid Access, Invalid Access Attempt, and Trace conditions, the System shall be capable of logging the following information as a minimum: Door name and number; card number; and cardholder name (If truncated, shall be 12 characters minimum). For Invalid Access Attempts, the System shall display and log reason for rejection.

I. The System at a minimum shall log all Monitor Point and Alarm Condition activity.

J. All System Operator commands from Operator Workstation shall be logged, including Unlock, Re-lock, Arm, Disarm, Disable, Silence, Acknowledge, Reset, and other such System Operator commands. Log of Operator commands shall identify the System Operator who issued each command. The System shall log unauthorized attempts to gain access to the System, such as the use of an invalid password, including the terminal node and/or network address from which the attempt was made.

K. The System shall log all automatic System operations that occur by Time Code, including Unlock, Re-lock, Arm, Disarm, and other such timed operations.

L. All System failures shall be logged including Hardware Failure, Communications Failure, Power Fail, and other such System conditions.

M. All System Operator configuration activity, such as modification to Clearance Codes, Time Codes, Monitor Points, Cardholder Records, and other System data, shall be recorded to an operator audit log. As a minimum, the operator audit log shall identify the type of data that

was modified, old data, new data and identify the System Operator who modified it. The System shall allow the Audit report to be filtered by date and by System Operator.

N. System shall be capable of selectively displaying all System configuration data at an Operator Workstation screen, allowing the viewing of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Device Groups/Areas, and other configuration data. System shall provide ability for System Operator to selectively view specific types and numerical ranges of data all based on their user assigned operator profile.

O. System shall be capable of printing all System configuration data to printer, allowing print-out of Cardholder Records, Clearance Codes, Doors, Time Intervals, Time Codes, Monitor Points, Door Groups, Device Groups/Areas, and other configuration data. System shall provide ability for System Operator to selectively print specific types and numerical ranges of data all based on an operator's assigned operator profile.

2.32 ARCHIVAL STORAGE AND BACK-UP FEATURES

A. System shall provide capability to backup all System and database files, including cardholder database, to the local computer or external/network device. System shall provide a menu-driven backup and restore capability, with operator prompts, enabling backups and restores to be made while the SMS application program is running. The System shall allow for configurable days and times for the backup to automatically occur.

B. Backups shall be capable of being initiated from any Operator Workstation. Backup capability shall be available without requiring that the SMS application be closed and making backups shall not interrupt System operation or require restarting of the SMS host computer.

C. System shall provide for archival transfer of event data from hard disk to CD. Archival transfer shall load event data to the local drive or external / network location and shall clear event data from the on-line System Journal file after verifying good archive copy. System shall provide a menu-driven utility to allow archival transfer. The System shall allow for configurable days and times for the archive process to occur automatically.

D. The System shall permit archival storage and back-up to external storage devices via the Users network.

2.33 DATABASE RETRIEVAL FEATURE

A. The System shall provide an integrated database retrieval for archive. The Database retrieval shall provide search and retrieval capabilities to allow selective reporting of past events from hard disk.

B. The System shall provide basic search tools to allow selective retrieval of events according to criteria established by System Operator. As a minimum, search tools shall allow selective recall of events by type, time frame, location, cardholder name, and card number. Basic search tools shall be usable by non-technical people who have received a minimal amount of training. Basic searches shall not require knowledge of any type of programming language.

C. In addition to basic search tools, the database retrieval System allows the use of Structured Query Language (SQL) to conduct more advanced searches. The SQL used shall be an industry-standard type that is in common use. SQL queries shall permit access to all data stored in System Journal and well as all data in System configuration database including Cardholder Records.

D. Database retrieval reports shall be capable of being printed to designated printers upon operator command. Retrieval of data shall not interrupt System operations.

E. System shall allow database retrieval reports to be exported in industry standard data formats capable of being exported into external spreadsheets, databases, and report analysis tools.

F. System shall provide a menu-driven utility that allows the retrieval of journal data from archival CDs, for the purpose of generating reports. Retrieval, reporting, and viewing of data from CD shall not interrupt System operation or require that the current event data be cleared from hard disk.

2.34 PHOTO IDENTIFICATION BADGE SYSTEM

A. The System shall provide photo identification badge capabilities which shall allow the design, production, and management of photo identification badges for Employees and Vendors. Within this Specification, the photo identification badge System shall be defined as the "Badging System".

B. The Badging System shall be a software module that is seamlessly integrated within the SMS software application program. Badging System software must operate on SMS host computer and use SMS Operator Workstations for badge production and verification.

C. The Badging System shall store photo image and other badge information for each Cardholder Record.

D. The Badging System shall provide full-featured badge design and production capabilities. The Badging System shall permit the user to create an unlimited number of badge designs and store them as reusable badge templates. Systems that require that badge templates be created or modified by manufacturer are not acceptable.

E. As a minimum, the Badging System editor shall:

1. Permit badge layouts to be designed with either vertical or horizontal badge orientation.
2. Permit insertion, sizing, and placement of photo images on badge layout.
3. Permit insertion, sizing, and placement of text boxes within badge layout. Two types of text boxes shall be available; field text boxes which insert variable text from a selected field within the Cardholder Record, and label text boxes which produce fixed text.
4. Permit use of any standard Windows True type font in point sizes between 4 and 48 points. Text shall be capable of being formatted as normal, bold, italic, and bold italic.
5. Permit use of both uppercase and lowercase text characters within a text box.
6. Permit use of both vertical and horizontal text on badge, irrespective of badge orientation.
7. Provide text justification within text boxes. Types of justification shall include right-justification, left-justification, and centered.
8. Permit text boxes to be defined for "scale-to-fit" formatting, where text size is automatically adjusted to accommodate available space within text box.
9. Permit use of standard Windows colors for text, text box background, badge background, photo background, signature, signature background, and borders.
10. Permit the import, sizing and placement of graphic images (such as logos) on the badges and shall accept images in standard graphics formats such as .JPG, .BMP, .GIF, etc.

11. Permit the assignment of aspect ratio to imported images.

F. The Badging System shall permit the use of signatures on badges. The Badging System shall permit the capture of signatures using any electronic signature pad which utilizes standard WINTAB device drivers.

G. The Badging System shall permit the use of any badge printer that utilizes standard Windows printer drivers. If supported by the printer the Badging System shall permit double-sided printing. If supported by printer, Badging System shall permit edge-to-edge printing on card.

H. Badging System shall permit the capture of color photographic images from any of the following sources:

1. Direct video source, such as live video camera, connected to video capture board installed in any Operator Workstation.
2. Scanned image from any standard TWAIN-compliant scanner supported by Windows.
3. Image file in standard .JPG format from digital camera or another source.

I. The Badging System shall provide a "print preview" feature which allows badges to be viewed in a "what-you-see-is-what-you-get" (WYS IWYG) mode prior to being printed.

J. The Badging System shall provide the ability to batch print a group of badges based on the cardholders filtered in Personnel Manager.

2.35 QUICK LOOK-UP FEATURE

The System shall provide a method to quickly display the cardholder record and photo image for any cardholder based on cardholder name. This feature shall be available to authorized operators at any Operator Workstation.

2.36 AUTOMATIC DISPLAY OF PHOTO IMAGE

A. The System shall allow the user to assign automatic image display on the "Event Manager" screen where an authorized operator is logged on.

B. From the "Event Manager" screen an authorized operator shall be capable of selecting, using a single mouse click a reader access display or access the cardholder's file.

2.37 INTELLIGENT CONTROLLER

A. The system shall support a number of intelligent controllers and smart reader/locks as called out in section 1.04 subsection 4. They shall follow an open standards protocol OSDP and shall be available from multiple vendor suppliers. Controllers requiring special flash support to work with a SMS shall not be acceptable.

B. The "Intelligent Controllers" shall be field panels that provide local processing and control of all access control, alarm monitoring, and auxiliary control functions. Intelligent Controllers shall typically be located within equipment closets throughout the user's site or sites. They shall be UL 294 listed and in special cases Plenum rated.

C. The Intelligent Controllers shall provide full-featured card access control processing without requiring communication with SMS host computer and operate in a fully distributed manner. All data necessary for card processing shall be stored within memory of Intelligent Controller. Communication with the SMS host computer shall not be required to process card access requests or other assigned control functions.

D. The Intelligent Controller Operating System, firmware, application program, and database shall be stored in solid-state memory media such as EEPROM, RAM, ROM. The Intelligent Controller shall not use any type of disk drive (hard drive, floppy drive, CD, or optical drive) to support normal operations.

E. The application firmware imbedded in the Intelligent Controller shall be field-upgradeable to permit system enhancements to be made as they become available from the manufacturer. The firmware provided in the Intelligent Controller shall be the latest version released by the Manufacturer at the time of installation. Providing an earlier version of firmware than identified by the manufacturer not being their latest version release shall be viewed as Non-Compliant.

F. Intelligent Controllers shall utilize "Flash ROM" that permits upgrades to be made automatically by download from SMS host computer.

G. The System shall support a means to download firmware upgrades as a standard and shall not be dependent on the manufacturer or site integrator to maintain firmware for the Intelligent Controllers.

H. Intelligent Controllers and smart reader/locks shall be equipped with an integral real-time clock. Intelligent Controllers shall be capable of processing timed control functions (such as automatic unlock) without requiring communication with SMS host computer.

I. Intelligent Controllers shall be capable of processing local alarm input/output events (such as operation of local audible alarm horn when Monitor Point is activated) without requiring communication with the SMS host computer. The System shall be capable of communicating to these Intelligent Controllers using all the following methods:

    1. Over User's TCP/IP network. A native implementation of TCP/IP, where the Intelligent Controller is directly connected to the internet is preferred.

J. Intelligent Controllers shall provide the capacity to control a minimum of two readers. Smart reader locks shall have the same capability but manage a single reader.

K. Each Door defined and managed by an Intelligent Controller shall be configured with one card reader input, one SPDT (Form C) lock output, one supervised door switch input for Door position detection (Forced or Held open monitoring), and one Request-To-Exit (REX) input.

L. Intelligent Controller shall provide a memory capacity for not less than 5,000-access cards, with the selected processor they shall be capable of expandable to a minimum of 30,000-cards.

M. The Intelligent Controller shall permit access of cards not in local memory upon validation of access request by SMS host computer and upload the card information in to local memory once authorized by the SMS host.

N. The Intelligent Controller shall rapidly process all local access control transactions. The time between presentation of a valid card at card reader until the time that door unlocks shall not exceed 500 milliseconds under worst-case conditions.

O. The Intelligent Controller shall link with I/O modules for input monitor points, and relay-controlled outputs.

P. Intelligent Controller shall utilize an industry standard Wiegand and Magnetic Swipe or RS485 ODSP protocol to connect with the specified card readers, permitting the use of multiple reader technologies and other data collection devices. Intelligent Controllers that

rely exclusively on a “proprietary” card reader protocol that requires the use of any specific manufacturer’s card reader or input device shall be viewed as Non-Compliant.

Q. The Intelligent Controllers shall support the use of Wiegand formats of varying bit lengths from 26 bit to 64 bit. The Intelligent Controllers shall permit the intermixing of Wiegand card formats as well as other reader technology formats like Mag-Stripe encoding.

R. Based on the reader technology the selected the Intelligent controllers shall allow the user to present or insert a card at a reader and the System, if the format of the card is stored in a System level library, shall identify the format and list specific detail allowing the user to define the card format in the Intelligent Controller for site use.

S. The System shall display all access requests with descriptions to assist a user in defining a card format into the System or selecting existing formats from a pre-defined library of formats, to include Wiegand, Smart card and Mag-stripe.

T. The Intelligent controllers shall allow a minimum of 8 card formats to be stored locally for user assignment. Smart reader locks shall support up to three at a minimum.

U. The Intelligent Controllers shall be provided power either via a POE device or via a power supply with standby battery. Batteries shall be sized to provide a minimum of eight hours of full standby operation in the event of primary power failure. The Intelligent Controllers shall report loss of primary AC power to SMS host within 10 minutes of power failure. The Power supplies shall be Underwriters Laboratories (UL) listed. The Power supply may be integral to Intelligent Controller or may be furnished within a separate enclosure.

V. In the event of communications failure to the SMS host computer, the Intelligent Controllers shall store access control and alarm monitoring transactions in a memory buffer. Minimum size of memory buffer shall be 30,000-transactions. When communication is restored, Intelligent Controller shall automatically upload the stored transactions to SMS host computer.

W. The Intelligent Controller shall be capable of operating in a temperature range of from -40° C to +75° C, (operating) with humidity at: 10% to 95% RHN.

2.38 INTERFACE TO VIDEO SYSTEM

A. The System shall provide a software level integration to the Video Management Systems. The video management system of choice shall be Video Insight as manufactured by Panasonic with no equivalent. All integration should include items 1 and 2 below and depending upon video system type, one or more from items 3 - 5 listed below.

B. Live Video Call-Up from the Hardware Device Tree for any IP based camera.

C. Plot cameras onto graphic maps to call up Live Video for any IP based camera.

D. Selection of specific cameras upon receipt of command from Physical Security Information Management System.

E. Activation and positioning of PTZ camera “presets” upon receipt of command from Security Management Software.

F. Automatic activation of video recording System upon receipt of command from Security Management Software.

2.39 PRODUCTS, GENERAL

All equipment provided shall be compatible with the Imron headend/software. Verify compatibility of all components specified prior to submitting a proposal.

2.40 STANDARD COMPUTER EQUIPMENT

A. "Standard Computer Equipment" is industry-standard personal computer equipment that is to be used in conjunction with the Security Management Software.

B. "Standard Computer Equipment" includes personal computers and their related components, including memory, hard disk drives, floppy disk drives, tape drives, CD-ROM drive, video board, keyboard, monitor, mouse, and network interface card. Personal computers shall be used as a platform for the SMS Host Computer and Operator Workstations.

C. To maintain compatibility all Standard Computer Equipment provided for this project contact the manufacture for minimum PC specifications: Note: All associated computer peripherals shall be provided, video terminals, keyboards, mouse, rails, etc.

2.41 SECURITY MANAGEMENT SOFTWARE HOST COMPUTER ("SERVER")

A. Provide Standard Computer Equipment for SMS host computer in accordance with Paragraph 2.02.

B. Provide internal CD Rewritable (CD-RW) drive to facilitate data back-up. Drive shall be capable of using both CR-R and CD-RW disks. Minimum speed: 24X write, 24X rewrite, 32X read.

C. Provide Security Management Software application software for SMS host computer ('server'). Software shall provide all Security Management Software's features, capabilities, and capacities as set forth in Part 1 of this specification. Provide security key (dongle) type required for the server. Only the server shall require a dongle. Systems that require security keys for all clients shall be viewed as Non-Compliant

D. Provide Microsoft Windows based Server operating System, latest version supported by Security Management Software.

E. Provide all third-party database software (such as SQL server) if needed for System to operate as specified.

F. Provide all device drivers and utility software needed for the System to operate as specified. Utility software shall include but shall not be limited to import/export utilities, report generators, data conversion utilities, network utilities, and communications utilities.

G. Provide virus protection and firewall software to provide security of SMS application software and data as required by the SMS.

H. Where the SMS application software does not provide integral map Drawing tools, provide all third-party graphics and conversion programs necessary to create and edit graphic maps as specified.

I. Provide licenses for all specified software, including databases and other third-party software. Licenses shall be provided in quantities as necessary to support simultaneous use of all specified SMS Operator Workstations.

J. All software shall be provided on CD (compact disk). Original copies of all software shall bear the manufacturers label and serial number. After installation, original copies of software shall be provided to Owner.

2.42 COMMUNICATIONS ACCESSORIES

A. Provide all communications accessories needed to connect host computer to Intelligent Controllers, smart reader/locks and other equipment as indicated. All devices shall be as recommended and approved by the manufacturer of the Security Management Software.

B. Provide all cables, connectors, adapters, hubs, switches, converters, buffers and other communications accessories necessary to properly interconnect System components.

2.43 PHOTO IDENTIFICATION BADGE SIGNATURE PAD

A. Provide tablet input device ("signature pad") for capturing signatures for photo identification badges. Minimum size of signature gathering area to be 60 cm x 30 cm. Signature pad shall use pressure-sensitive technology which allows the use of any standard pen and shall not require the use of an electronic stylus. Shall connect to computer using RS-232 or USB connection.

B. Signature pad to be fully compatible with Security Management Software. Provide device drivers and all other hardware and software needed to use signature pad with proposed Security Management Software.

2.44 PHOTO IDENTIFICATION BADGE PRINTER AND ACCESSORIES

A. Heavy-duty, high-speed identification card printer: Full-color badge printer for direct print on proximity cards.

B. Provide with software TWAIN compatible drivers for Windows.

C. Provide printer with a complete set of ribbons as called out to meet initial card production.

D. Provide with manufacturer's recommended cleaning kit.

E. Provide printer with table-top slot punch to allow punching of proximity cards in horizontal or vertical direction. Punch to be factory calibrated for vertical punching.

2.45 INTELLIGENT CONTROLLERS

A. Provide Intelligent Controllers in locations indicated on the Drawings. Intelligent Controllers shall provide all Security Management Software features, capabilities, and capacities as set forth in this Specification.

B. Provide all wiring harnesses, connectors, and cabling required to properly interconnecting Intelligent Controller boards and accessories.

C. Where Intelligent Controller is not powered by a POE device the integrator shall supply a power supply, that is U.L. listed in accordance with Security Management Software Manufacturer's Requirements. External power supply used to power Intelligent Controller may be combined with Auxiliary Power Supplies specified below so long as equivalent auxiliary power capacity is provided (combined power supply should provide all power needed to supply Intelligent Controller, plus provide rated capacity of specified Auxiliary Power Supply).

D. A minimum of one Intelligent Controller providing the capabilities and capacities as indicated herein shall be provided where specified. Provide additional Intelligent Controllers and card reader boards, as needed to fully support field devices connected to the controller.

2.46 MANUAL DOOR RELEASE BUTTON — DESK MOUNTED

Manual release button in surface mounted enclosure. Suitable for mounting to desk or counter. Momentary operation. DPST contacts rated at 3-amp.

2.47 MANUAL DOOR RELEASE BUTTON —WALL MOUNTED

Manual release button on single-gang plate. Suitable for mounting to wall. Momentary operation. All steel momentary push button with SPDT contacts rated at 3-amp.

2.48 PILOT RELAYS

A. Provide pilot relays where current Requirements of device being controlled exceeds rating of Intelligent Controller relay contact output or where electrical isolation is required.

B. Provide pilot relays at security backboard for card reader lock outputs.

C. Provide pilot relays at locations where indicated for interface connections to power boosters, automatic doors and gates, fire alarm Systems, and other external equipment.

D. Relays shall be heavy-duty industrial grade approved. 24 VDC coil, contacts rated at no less than 5-amp at 28 VDC.

E. Provide screw-terminal relay sockets for each relay.

2.49 SYSTEM DOCUMENTATION

A. Provide online, context searchable help instructions and manuals available 24 hours a day 7-days a week.

B. Online help should allow for language translation and the ability to be printed or e-mailed directly from the online help system all other systems without this functionality will be considered non-compliant.

PART 3 - EXECUTION

3.01 QUALITY ASSURANCE

A. Contractor shall be a factory authorized Reseller / Installer of all major components installed as a part of this project. Contractor shall submit proof of such authorization as a part of their bid package.

B. Contractor shall have successfully completed a minimum of three projects similar in size and scope to this one and shall submit references for such projects with their bid package. Reference shall include project name, location, type of facility, system(s) installed, and end-user contact information. It is expected that substantially the same personnel will be assigned to this project as participated in the referenced projects. This would include the Project Engineer, Project Manager, and Lead Installation Technician. If any of these Personnel were not involved in the referenced project, Contractor shall supply resumes for these employees documenting their experience and qualifications related to this project.

C. At a minimum, the Lead Installation Technician assigned to this project shall be Manufacturer certified in the installation of all major components installed as a part of this project.

D. IP-Enabled access control products are required to be supplied and installed only through designated ASSA ABLOY "Authorized Channel Partner" (ACP) and “Certified Integrator” (CI) accounts and IMRON authorized Dealers. List of ASSA ABLOY and IMRON approved Vendors.

1. Red Rock: Randy Jara 714-475-9230 randyj@itredrock.com
2. Wachter: Geoff Colley 619-315-8796 Geoff.colley@wachter.com
3. Johnson Controls: Kathy Roberts 858-248-3589 Kathleen.V.Roberts@jci.com

E. Pre-Submittal Conference: Conduct coordination conference in compliance with Requirements in Division 01 Section "Project Meetings" with attendance by representatives of Supplier(s), Installer(s), Systems Integrator(s), and Contractor(s) to review proper methods and procedures for receiving, handling, and installing door and access control hardware to Manufacturer's recommendations and according to Specifications.

1. Prior to installation of door hardware, arrange for Manufacturers' Representatives to hold a project specific training meeting on the proper installation and adjustment of their respective products. Product training to be attended by the Installers of access control hardware for the aluminum, hollow metal and wood door sections. Training will include the use of installation manuals, hardware schedules, templates and physical product samples as required.
2. Inspect and discuss electrical roughing-in, power supply connections, and other preparatory work performed by other trades.
3. Review sequence of operation narratives for each unique access-controlled opening.
4. Review and finalize construction schedule and verify availability of materials.
5. Review the required inspecting, testing, commissioning, and demonstration procedures.

3.02 COORDINATION

A. Coordinate quantity and arrangement of assemblies with ceiling space configuration and with components occupying ceiling space, including structural members, pipes, air-distribution components, raceways, cable trays, recessed lighting fixtures, and other items.

B. Integrated Access Control Door Hardware and Electrical Coordination: Coordinate the layout and installation of scheduled integrated access control door hardware, and related access control equipment with required connections to source power junction boxes, power supplies, detection and monitoring hardware and fire alarm system.

1. Door Hardware Interface: The access control system to interface and be connected to electrified and integrated access control door hardware as described under Division 08 Sections "Door Hardware" or “Access Control Door Hardware". Coordinate the installation and configuration of electrified door hardware being monitored or controlled with the controls, software and access control hardware specified in this Section.

C. Templates: Obtain and distribute to the parties’ involved templates for doors, frames, and other work specified to be factory prepared for installing electrified door hardware and access control system components. Check Shop Drawings of other work to confirm that adequate provisions are made for locating and installing access control system hardware to comply with Indicated Requirements.

D. Door and Frame Preparation: Related Division 08 Sections (Steel, Aluminum and Wood) doors and corresponding frames are to be prepared, reinforced and pre-wired (if applicable) to

receive the installation of the specified electrified, monitoring, signaling and access control system hardware without additional in-field modifications.

3.03 SITE SPECIFIC SCOPES OF WORK

A. Procure, provide, install and configure for full functionality all PACS components as shown on the Project Drawings and described within these specifications.

B. For any door not called out as an access control door, Contractor shall install an empty 2-inch conduit terminating in a 12 x 12 x 4-inch junction box mounted above the non-access-controlled door

C. Program integration between the Imron PACS elements and the Video Insight Surveillance elements to tag video associated with the following events:

1. Forced door
2. Door left ajar
3. Invalid card presented five or more successive reads
4. Intrusion device activation

D. For any telecom runs in excess of 300-foot, place an intermediate termination point at the 290-linear foot mark on the cable, prior to any datacom / PoE extenders as to maintain the cable plant warranty up to the intermediate termination point.

1. Electrical contractor, Division 26, to provide the following:

a. Source power wiring (120VAC) as required for the integrated locking and access control hardware, equipment, accessories and power supplies. This includes quad outlets as required on a dedicated circuit in the designated IT/Telecom room(s) and the related conduit, stub-in, junction boxes and connectors required for the source power delivery and connections.

b. Provide required conduit, stub-in, junction and back boxes for both the electrified locking hardware and access control equipment at each of the access controlled or monitored openings per plan Drawings and specs. Supply and install conduit between each of the aforementioned devices and between the electrical junction boxes, power supplies and access control equipment located on or above the door opening.

1) At wall mounted remote readers, provide conduit on the secured side of the door, 36-inches from the finish floor and 6-inches from the edge of the frame to the related power supplies and access control equipment.
2) At electrical hardware power transfers provide conduit on the secured side of the opening from the power transfer, thru-wire hinge, or serviceable panel location on the frame jamb to the related power supplies and access control equipment.

E. Electrical Contractor to provide all 120VAC cabling connections and terminations from the electrical junction boxes to these electrical devices

3.04 EXAMINATION

A. Examine pathway elements intended for Category 6A cabling. Check raceways and other elements for compliance with space allocations, installation tolerance, hazards to camera installation and/or operation, and other conditions affecting installation.

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

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.05 WIRING

A. Comply with Requirements in Section 26 05 33 "Raceways and Boxes for Electrical Systems."

B. Wiring Method: Install cables in raceways and or conduit unless otherwise indicated.

1. Except raceways are not required in accessible indoor ceiling spaces and attics, where Contractor shall utilize self-supported J-hooks.
2. Except raceways are not required in hollow gypsum board partitions.
3. Conceal raceways and wiring except in unfinished spaces.

C. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points with no excess and without exceeding manufacturer's limitations on bending radii. Provide and use lacing bars and distribution spools.

D. Splices, Taps, and Terminations: For power and control wiring, use numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures. Tighten electrical connectors and terminals according to Manufacturer's published torque-tightening values. If Manufacturer's torque values are not indicated, use those specified in UL 486A-486B.

E. For LAN connection and fiber-optic and copper communication wiring, comply with:

1. Section 27 13 13 "Communications Copper Backbone Cabling"
2. Section 27 13 23 "Communications Optical Fiber Backbone Cabling"
3. Section 27 13 33 "Communications Coaxial Backbone Cabling
4. Section 27 15 00 "Communications Horizontal Cabling."

F. Grounding: Provide independent-signal circuit grounding recommended in writing by Manufacturer.

3.06 PHYSICAL ACCESS CONTROL SYSTEM INSTALLATION

A. PACS device locations shown on Drawings are approximate, and Contractor shall verify final position with the Owner before any work is done.

B. Install all PACS components per manufacturer’s installation instructions.

C. Install headend / software at location(s) as directed by the Owner.

D. Install key locks on any field enclosures

E. Identify system components, wiring, cabling, and terminals according to Section 26 05 53 "Identification for Electrical Systems."

3.07 FIELD QUALITY CONTROL

A. Manufacturer's Field Service: Engage a factory-authorized Service Representative to inspect, test, and adjust components, assemblies, and equipment installations, including connections.

B. Tests and Inspections:

1. Inspection: Verify that units and controls are properly installed, connected, and labeled, and that interconnecting wires and terminals are identified.

2. Pretesting: Align and adjust system and pretest components, wiring, and functions to verify that they comply with Specified Requirements. Prepare PACS equipment for acceptance and operational testing as follows:
    a. Prepare equipment list described in "Informational Submittals" Article.
    b. Verify operation of all card readers and door locking hardware.
    c. Verify operation of request-to-exit sensor, door position sensor, and local door controller
    d. Verify proper operation of workstation with PACS headend / software for logging alerts and events
    e. Verify all integration functionality with Surveillance System and IDS.
3. Performance Verification Test Schedule: Schedule tests after pretesting has been successfully completed and system has been in normal functional operation for at least 14 days. Provide a minimum of 14 working days' notice of test schedule.
    a. Contractor shall prepare and submit to the Owner a PVT Plan showing a structured and complete testing procedure. This PVT Plan shall be submitted to the Owner a minimum of 14 working days prior to planned start of testing.
    b. PVT Plan shall show equipment being tested, means of testing, and pass/fail criteria.
    c. PVT form shall include space for Contractor/Owner initials on each testing phase, along with a signature page with PVT results and follow-up notes.
4. Should any component of the system fail TWO consecutive PVT tests, the Contractor shall be liable for costs incurred by the Owner to provide personnel for further PVT testing.

C. Physical access control system will be considered defective if it does not pass tests and inspections.

D. Prepare test and inspection reports.

3.08 ADJUSTING

A. Occupancy Adjustments: When requested within 12 months of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions. Provide up to TWO visits to Project during normal business hours for this purpose. Tasks shall include, but are not limited to, the following:
    1. Check cable connections.
    2. Check proper operation of readers and doors.
    3. Check proper operation of all integration driven functionalities.

3.09 CLEANING

A. Clean installed items using methods and materials recommended in writing by Manufacturer.

B. Clean PACS components as needed.

3.10 TRAINING

A. Training on the surveillance system shall be as follows:

1. User Training - Contractor shall provide a total of 16 hours' user training as follows:

a. 4-hours' initial user training to be provided after successful PVT and just prior to final system acceptance.

b. 4-hours' administrator training to be provided after successful PVT and just prior to final system acceptance.

c. 2-hour refresher user trainings, at 30 and 60 days after the initial user training session.

d. 2-hour refresher administrator trainings, at 30 and 60 days after the initial administrator training session.

e. 2-hours' initial preventative maintenance training to be provided after successful PVT and just prior to final system acceptance

f. 1-hour refresher preventative maintenance training to be provided 60 days after the initial preventative maintenance training

END OF SECTION 28 13 02
093022/212278